NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE SYSTEM ENGINEERING APPROACH: TAIWAN NAVY INCORPORATION OF MOBILE DEVICES (SMARTPHONE) INTO ITS FORCE STRUCTURE

by

Wei-yang Lee

June 2015

Thesis Advisor: Raymond Buettner
Co-Advisor: John Gibson

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE June 2015	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE THE SYSTEM ENGINEERING APPROACH: TAIWAN NAVY INCORPORATION OF MOBILE DEVICES (SMARTPHONE) INTO ITS FORCE STRUCTURE		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Wei-yang Lee			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Attempting different approaches to explore the best practice of optimizing mobile security and productivity is necessary to improve the Taiwan navy's maneuverability and capability in the information age. This thesis uses a system engineering approach to research various mobile security technologies and applications that can provide the Taiwan navy with appropriate smartphone systems to develop a secure and productive smartphone incorporation plan. Having addressed system requirements, considered stakeholders' concerns, and analyzed commercial off-the-shelf products, preliminary results have shown that Apple iOS is the most secure and productive system for smartphone incorporation in the Taiwan navy. Before rolling out a comprehensive incorporation plan, it is essential to evaluate the recommended technologies through a pilot program that simulates realistic naval activities to further correct deficiencies and determine the feasibility of the selected technologies. The intent of this research is to convince the Taiwan navy that secure smartphone incorporation is achievable through leveraging appropriate smartphone technologies and corresponding strategy, policy, and training.

14. SUBJECT TERMS smartphone security, enterprise mobility, mobile device incorporation, system engineering approach, Taiwan navy			15. NUMBER OF PAGES 113
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

THE SYSTEM ENGINEERING APPROACH: TAIWAN NAVY INCORPORATION OF MOBILE DEVICES (SMARTPHONE) INTO ITS FORCE STRUCTURE

Wei-yang Lee
Lieutenant, Taiwan Navy
B.S., United States Naval Academy, 2010

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEM ENGINEERING

from the

**NAVAL POSTGRADUATE SCHOOL
June 2015**

Author: Wei-yang Lee

Approved by: Raymond Buettner
                 Thesis Advisor

                 John Gibson
                 Co-Advisor

                 Dan Boger
                 Chair, Department of Information Science

iii

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Attempting different approaches to explore the best practice of optimizing mobile security and productivity is necessary to improve the Taiwan navy's maneuverability and capability in the information age. This thesis uses a system engineering approach to research various mobile security technologies and applications that can provide the Taiwan navy with appropriate smartphone systems to develop a secure and productive smartphone incorporation plan. Having addressed system requirements, considered stakeholders' concerns, and analyzed commercial off-the-shelf products, preliminary results have shown that Apple iOS is the most secure and productive system for smartphone incorporation in the Taiwan navy. Before rolling out a comprehensive incorporation plan, it is essential to evaluate the recommended technologies through a pilot program that simulates realistic naval activities to further correct deficiencies and determine the feasibility of the selected technologies. The intent of this research is to convince the Taiwan navy that secure smartphone incorporation is achievable through leveraging appropriate smartphone technologies and corresponding strategy, policy, and training.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
BBM	BlackBerry Messenger
BES	BlackBerry Enterprise Server
BGAN	Broadband Global Area Network
BS	base station
BYOD	Bring Your Own Device
C2	command and control
CAC	common access card
CEO	Chief Executive Officer
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CNSS	Committee of National Security System
CO	commanding officer
COBO	Corporate Owned Business Only
COPE	Corporate Owned Personally Enabled
COTS	commercial off-the-shelf
CPU	central processing unit
CYOD	Choose Your Own Device
DAG	Defense Acquisition Guidebook
DISA	Defense Information System Agency
DOD	Department of Defense
DRAM	Dynamic random access memory
DTLS	Datagram Transport Layer Security
DT&E	developmental test and evaluation
DVD	digital video disc
ECDSA	Elliptic Curve Digital Signature Algorithm
EMM	Enterprise Mobility Management
FOC	Full Operational Capability
GEO	geostationary earth orbit
GPS	Global Positioning System

HAP	High Assurance Platform
HF	high frequency
HTS	High throughput satellite
ID	identification
IMSI	International Mobile Subscriber Identity
INCOSE	International Council on System Engineering
IOC	Initial Operational Capability
IP	Internet Protocol
ISO	International Organization for Standardization
IT	information technology
LOE	limited objective experiment
LTE	Long-Term Evolution
MAM	Mobile application management
MDM	Mobile device management
MEO	medium earth orbit
MS	mobile station
NAC	Network Access Control
NCC	National Communication Commission
NFC	Near field communication
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OEM	original equipment manufacturer
OOD	officer of the deck
OS	operating system
OT&E	operational test and evaluation
PC	personal computer
PLA	People's Liberation Army
POD	plan of the day
RAF	Royal Air Force
RAM	random access memory
RAND	random number
RFID	radio frequency identification

RoTs	Roots of Trust
RSA	Rivest-Shamir-Adleman
RTC	Root of Trust for Confidentiality
RTI	Root of Trust for Integrity
RTM	Root of Trust for Measurement
RTR	Root of Trust for Reporting
RTV	Root of Trust for Verification
SAG	surface action group
SATCOM	satellite communication
SD	Secure Digital
SE	System Engineering
SHA	Secure Hash Algorithm
SIM	subscriber identity module
SITREP	situation report
SMS	Short Message Service
SRES	signed response
SSL	Secure Sockets Layer
TCG	Trusted Computing Group
TLS	Transport Layer Security
TPM	Trusted Platform Module
UHF	ultrahigh frequency
USB	universal serial bus
VHF	very high frequency
VM	virtual machine
VoIP	Voice over IP
VP	virtual phone
VPN	virtual private network
VSAT	very small aperture terminal
WLAN	wireless local area network
WMAN	wireless metropolitan area network
WPAN	wireless personal area network
WWAN	wireless wide area network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

THIS PAGE INTENTIONALLY LEFT BLANK

I.   INTRODUCTION

The Taiwan navy maintains a great emphasis on information integrity, utilized to prevent adversaries from compromising information security. However, in doing so protection of information prevents users from smoothly operating in a modern network-centric environment, especially in mobile communications networks, and further impairs user productivity. According to various studies and surveys, 61% of information workers work outside of the office,[1] and more than 55% percent of respondents say mobile devices increase productivity.[2] More importantly, time is money. A 2013 report estimated that nine hours a week in productivity gain is equating to US$28 billion saved.[3] Due to its heavily fortified security protocols and disconnection from the World Wide Web and smartphone applications, the Taiwan military net lacks updated information and convenient functionality. Users rely on the military network only because it contains isolated work-related content such as personnel service records, administrative documents, executive orders, and logistic supply reports. This has severely undermined the Taiwan bc's productivity and caused it to fall behind other military organizations in the information domain.

A.   BACKGROUND

In response to the steady increase of smartphone usage among the troops, the Taiwan Ministry of Defense announced the smartphones management trial phase in January 2014.[4] Within the trial phase, selected units have the right to operate smartphone

---

[1] Citrix Systems, Inc., *Jump Start Mobile Productivity with MDM and Secure File Sharing*, (Fort Lauderdale, FL: Citrix), accessed February 11, 2015, https://www.citrix.com/content/dam/citrix/en_us/documents/oth/jump-start-mobile-productivity-with-mdm-and-secure-file-sharing.pdf.

[2] Ponemon Institute, LLC, *Security in the New Mobile Ecosystem* (Traverse City, MI: Ponemon Institute), August 2014, http://www.wincoil.us/media/89329/ponemon-raytheonsecurityinthenewmobileecosystemresearchreport.pdf.

[3] Mobile Work Exchange, *The 2013 Digital Dilemma Report: Mobility, Security, Productivity—Can We Have It All?* January 15, 2013, http://www.cisco.com/web/strategy/docs/gov/digital_dile_rep.pdf.

[4] Zongxian Xie, "Smartphone on Base Trial Verification and Control," *Youth Daily News*, January 4, 2014, http://news.gpwb.gov.tw/mobile/news.aspx?ydn=026dTHGgTRNpmRFEgxcbfcCSN9Fhd8KFbqLRgMWauV83KTHsQMjmV%2FQwBCVEb%2BKgPnpTj46r3NaVXND4iHNKfHfg3tQrsMnpfokazSjAL3k%3D.

devices on military installations, but with certain conditions. To ensure information security and military secrecy, each installation establishes "SMART Zones" (Red = Restricted, Yellow = Transition, and Green = Go) according to each unit's infrastructure and systems layout.[5] In addition to the "Smart Zones" management policy, cellphone users have to register their phones with the unit information management authority to receive authorization to use the phones. In Taiwan, the military Internet is physically separate from the civilian Internet, which means the Taiwan navy intranet does not reply on a virtual private network (VPN) or other Internet portals to authenticate intranet users. Under current information management guidelines, all USB ports and DVD slots are disabled, except those on designated "connector" computers.

The Taiwan military uses the "containment" approach to handle information security concerns. To enter the Taiwan navy intranet via smartphone, the user has to have access to military Internet "connector" computers or a Wi-Fi signal. According to the described security measures above, the military intranet Wi-Fi signal is a much higher risk vulnerability compared to the "connector" computers, which can require up to four security checks before gaining access. Although it is easier to access a Wi-Fi signal, it is still secure because the signal has been encrypted using a specially designed encryption system. Unless the intruder gains access to the "connector" computers or obtains the encryption code to decipher the Wi-Fi signal, breaking into the Taiwan navy intranet from outside is highly unlikely.

B.   PURPOSE

The purpose of this research is to analyze the current Taiwan Naval operational environment to construct the optimal smartphone incorporation plan. When the Taiwan Minister of Defense starts allowing the troops to bring smartphones onto the base, it creates a great opportunity for the Navy to reevaluate the role of its intranet and optimal integration of the smartphone into its force structure. Currently, the Navy still thinks of smartphone devices as non–work-related personal devices with multiple information security vulnerabilities. Although smartphones have proven vulnerable to information

---

[5] Ibid.

security threats, the vulnerability assessment should not undermine the potential use and benefits that the smartphone technology can bring to the Navy.

Taiwan is one of the biggest electronics manufacturing countries, and the Taiwan navy has strong industrial support related to smartphone technology. Although Taiwan is small, it is a population-dense nation with a high demand for cellular technology. However, the Taiwan military as a whole is reluctant to incorporate smartphone technology due to the security risk posed by China. Currently, most smartphone components are built in China, where the communist state is notorious for violating the integrity and intellectual property of electronic products. In August 2014, F-Secure, an online security and privacy company in Finland, showed that a Xiaomi (Beijing-based phone maker) RedMi 1S smartphone sent contact information and phone data back to Xiaomi's remote server.[6] In December 2014, Taiwan's National Communications Commission (NCC) announced that 12 major phone makers, including Xiaomi, were under investigation for violation of the Taiwan's Personal Information Protection Act.[7] Although the investigation later concluded that all tested smartphone models were compliant with the terms of the Taiwan's Personal Information Protection Act, NCC noted that there is no defined international standard for smartphone information security and it would develop a standard and a device certification program in the future.[8]

The Taiwan navy's biggest challenge is to find the fine balance between maximizing information efficiency while minimizing information security risk under the complicated and intertwined Cross-Strait relations. This study is to help the Taiwan navy to identify and approach this balance by using the system engineering approach.

---

[6] F-Secure Labs, "Testing the Xiaomi RedMi 1S," August 7, 2014, https://www.f-secure.com/weblog/archives/00002731.html.

[7] Eva Dou, "Taiwan Says Phone Makers Violating Privacy Rule," *Wall Street Journal*, December 5, 2014, http://www.wsj.com/articles/taiwan-says-phone-makers-violating-privacy-rule-1417702686.

[8] Ching-i Wang and Ted Chen, "NCC Clears 12 Smartphone Models in Security Check," Focus Taiwan News Channel, December 30, 2014, http://focustaiwan.tw/news/ast/201412300025.aspx.

C. SCOPE

This research focuses on potential smartphone system requirements and integration. The research looks into existing commercial off-the-shelf (COTS) smartphones and applications to meet these system requirements, as well as examine existing and developing network technologies to meet integration requirements. The intent of the research is to provide a realistic and potential solution as to how the Taiwan navy should approach incorporating smartphone devices, especially as an asset to increase communication survivability and agility. This thesis explores the answers to the following questions:

1. How can the Taiwan navy ensure information security and operation security while incorporating smartphones into the Taiwan navy maritime force structure?

2. How can smartphones help to improve the Taiwan navy maritime command and control (C2) capabilities and flexibilities?

3. What are the risks and benefits of smartphone incorporation in military organizations?

Additionally, this research also investigates the following emerging technologies as they might apply for the Taiwan navy:

1. Mobile device security/privacy application

2. Maritime mobility

According to the International Telecommunications Union's estimation, mobile-cellular penetration will reach 90% in developing countries and 121% in developed countries by the end of 2014.[9] In addition, according to the Cisco Visual Network Index, by 2019, 97% of the global mobile handset traffic will be done via smartphones.[10] Similar to the impact of the first affordable automobile, the Model T in 1908, 100 years

---

[9] International Telecommunication Union. *The World in 2014—ICT Facts and Figures*. (Geneva, Switzerland: ICT, April 2014), http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf.

[10] Cisco Systems, Inc., "Cisco Visual Networking Index : Global Mobile Data Traffic Forecast Update, 2010—2015," February 3, 2015, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.

later the smartphone has achieved a great impact on human society. The automobile allows humans to travel from point A to point B relatively fast and cheaply, while the smartphone allows humans to connect information from point A to point B in a relatively convenient, timely, and affordable manner. Today in the Information Age, information is power and the smartphone has become the hub of information. The organizations that manage the smartphone properly thrive, and those that do not wither.

It is slowly becoming inevitable that every organization, including the military, must adopt the smartphone and utilize it as a system in their respective environment. This research is designed to examine how a military organization, a closely guarded system, can safely and securely adopt the smartphone, an openly connected system, with limited, managed risk. Smartphone adoption will not only change the existing security measures system but will also modify long-standing human behaviors. The goal of this research is to identify the appropriate system requirements for smartphones to enter into a closely guarded system and investigate the impact it creates for overall system management.

This research uses a system engineering approach to identify the requirements, draft preliminary designs, and develop an incorporation plan. The end goal of this process is to provide the Taiwan navy with a complete and realistic plan for smartphone incorporation into its force structure with organizational culture and operational environment considerations considered.

D.   THESIS ORGANIZATION

The remainder of this thesis is organized as follows:

Chapter II discusses the current smartphone security measures both in software and hardware applications. This chapter also examines current smartphone usage policies and guidelines for the U.S. DOD and other countries in order to establish a complete understanding of a secure mobile ecosystem. Additionally, the chapter looks into the developing satellite and wireless communication technologies that are critical for smartphone incorporation in a maritime environment. The main purpose of this chapter is to establish technological knowledge about the smartphone security and maritime

5

mobility, as both are critical considerations for the Taiwan navy smartphone incorporation process.

Chapter III uses the system engineering approach to address the primary research question. First, it reviews the definition of system engineering to create a general understanding of why this approach is in use and why it is critical to the purpose of this thesis. Second, using the Vee model of the system engineering approach guideline, this chapter describes the concept of operations, identifies the system requirements, and creates the needed system design parameters. The concept of operations section addresses the organizational and user expectations as well as the definitions of the system-operating environment. Next, the system design section looks into existing COTS systems and ideal system designs. In addition, Chapter III covers the current technological limitations of smartphones and their associated networks.

Chapter IV outlines the basic framework of a limited objectives experiment, the Taiwan navy Smartphone Incorporation Pilot Program, to verify the recommended outcomes of the system engineering approach in Chapter III. The pilot program aims to reveal the smartphone's influence on security, productivity, cost, and user experience aspects in the Taiwan navy ashore, at sea, and during emergency operations through experimental data analysis. The end goal of this chapter is to assist the Taiwan navy to make justifiable assessment and determine the feasibility of the smartphone incorporation via quantitative measures gathered from the pilot program.

Chapter V provides the conclusion of this research. The first portion of this chapter discusses the practical insight to the future Taiwan navy smartphone incorporation plan based on the knowledge and results found through the research process. The chapter then revisits the objectives of this research to confirm they were properly addressed. Last, this chapter concludes the research by indicating the necessity of smartphone adoption while stating the potential future research areas for smartphone incorporation into military organizations and environments.

II.   TECHNOLOGIES REVIEW

In 2013, Symantec's Norton report showed the lack of awareness of mobile security risks is alarmingly high, with 57% of adults being unaware of a mobile security solution.[11] The purpose of mobile security is to protect portable/mobile computing devices from threats and vulnerabilities in a wireless network environment. While the "Bring Your Own Device" (BYOD) trend continues to grow, so does the associated mobile security risk. Research conducted by Checkpoint Software shows that the increasing use of mobile devices has increased the number of security incidents, especially ones involving privacy and the loss of sensitive data stored in a device.[12] This lost data includes items such as corporate email, customer data, and network login credentials. Therefore, analysis of mobile devices, especially smartphones, which are increasingly being embedded in daily life, is critical and urgent to increase the capability and awareness of mobile security for both software and hardware.

A.   GOAL OF MOBILE SECURITY (SMARTPHONE)

Before introducing the various technologies and products associated with smartphone security, it is important to understand the goals of smartphone security: content protection, theft deterrence, enterprise perspective, and entity authentication.[13] Each goal is interrelated to the others, and together, when appropriately addressed, they form a safe and secure environment for smartphone users. Content protection focuses on the integrity of the content stored in the devices; it protects contents from malicious modification and unauthorized access. Theft deterrence ensures complete device accessibility and availability to the authorized user; it allows the user to remotely control and lock the lost or stolen smartphone. Enterprise perspective means the full-time

---

[11] Symantec Corporation, *Internet Security Threat Report 2014* (Mountain View, CA: Symantec, April 2014), http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

[12] Dimensional Research, *The Impact of Mobile Devices on Information Security: A Survey of IT Professionals* (Sunnyvale, CA: Dimensional Research, June 2013), https://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf.

[13] Qualcomm Inc., "Snapdragon Security," accessed February 11, 2015, https://www.qualcomm.com/products/snapdragon/security.

protection of sensitive corporate data; it creates corporate networks where both employee- and corporate-owned devices can operate safely and securely. Entity authentication ensures rightful user identify; it uses various methods like passwords or biometrics to protect devices from unauthorized access.

B.   SMARTPHONE SECURITY LAYERS

In a mobile environment, information rarely remains in place for an extended period. It is highly mobile and transferrable across the entire IT infrastructure. Focusing solely on the smartphone, the information still constantly moves within the device across different layers that pose their own distinct security challenge and risk. To achieve the goals in smartphone security, it takes collaboration of a combination of various security measures in different device layers shown in Figure 1. Altogether, smartphone security has the following layers: server layer, hardware layer, operating system layer, application layer, and user layer.[14]
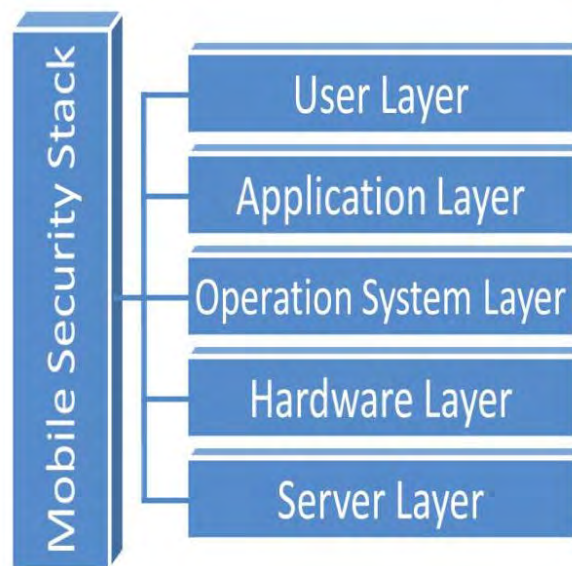
Figure 1.   Smartphone Security Layers

---

[14] Neil DuPaul, "Mobile Code Security," Veracode, accessed February 11, 2015, http://www.veracode.com/products/mobile-application-security/mobile-code-security.

The server layer may be regarded as the network security layer, which prevents malicious applications and attacks from reaching the targeted smartphones; it is the outermost layer in layered smartphone security architecture. The hardware layer deploys security measures at device component and firmware level such as Roots of Trust (RoTs), trusted execution environment, and secure subscriber identity module (SIM) authentication where malicious manipulations are unlikely. The operating system (OS) layer connects the hardware and application layers where the regular OS update is the main defensive mechanism to ensure safe and secure connection between the hardware and application layers. The application layer is where most mobile security incidents take place; similar to human skin where bacteria resides and breaks through into our immune system, the malicious software does the same at the application layer. The common security approaches at this layer are the applications review and mobile security/antivirus products. Last, the user layer, which takes the context out of computer science and into the realm of social science, implements mobile security through education and training.

Currently, the Taiwan navy intranet is a closed network with no authorized wired (tethered) or wireless smartphone connections. Therefore, the smartphone security concerns to the Taiwan navy intranet resource do not exist in the server layer. The Taiwan navy surface combatants do not regularly conduct long distance and long-term deployments, which means most of the ships spend equal amounts of time in port and at sea. The key difference between these two operating conditions is the availability of a cellular signal, which potentially connects the military domain to the public domain.

C. SMARTPHONE SECURITY SOLUTIONS

The foundation of a safe and secure smartphone system is a combination of both software- and hardware-based security solutions that can reach the goals of mobile security through the different mobile security layers. Although the software- and hardware-based solutions have the same smartphone security goals to achieve, both solutions are inherently different in many ways such as design consideration, interoperability, and performance.

1.   Software-Based Smartphone Security (Third Party)

Considering most smartphone users are not involved in smartphone design and development process, we don't include the Original Equipment Manufacturer (OEM) security solutions as part of software-based (third-party) security solutions which are more accessible and well known to the users. Several reports state that the software-based smartphone security market is set to grow to 3.4 billion by 2018, compared to 2.3 billion of the hardware-based market. [15] The increasingly popular BYOD trend in major organizations and the convenience of developing software are the core reasons that software-based solutions dominate hardware-based solutions in the global mobile security market.

Looking into the current smartphone security software, we identify three common practices: remote control, application-level security, and antivirus/firewall. These three practices rely on either preinstalled or third-party applications to perform security-related actions.

a.   *Remote Control*

This function is possible because of the cloud or so-called web-based technologies. The basic flow to enable the remote functions in the smartphone is to download the application and login onto its web-based management center. Upon login, the application starts transmitting device data to the server, which allows the user to remotely control the device through an Internet portal. Remote security functions have thrived due to the emerging cloud-computing trend in recent years, which mainly addresses the lost and stolen device issue. According to *Consumer Reports*, in 2013 more

---

[15] David M. Wheeler, "Smartphone Security—A Holistic View of Layered Defenses," SecureComm, Inc., accessed February 11, 2015, http://www.securecommconsulting.com/downloads/ NPS_Presentation_on_Smartphone_Security.pdf; Infonetics Research, "Infonetics Projects Mobile Device Security Software Market to Reach $3.4 Billion in 2018," April 25, 2014, http://www.infonetics.com/pr/ 2014/2H13-Mobile-Security-Client-Software-Market-Highlights.asp.; Brian Robinson, "Hardware-Based Mobile Security Market Heats up," *Government Computer News*, February 10, 2014, http://gcn.com/ articles/2014/02/10/mobile-hardware-security.aspx?admgarea=TC_Mobile.

than three million smartphones had been lost or stolen in the United States.[16] The remote control functionality allows the owners or organizations to track, lock, wipe, backup, and kill the lost or stolen device to prevent unauthorized access to sensitive information. However, the remote control works only when the device connects to the Internet, which leaves open the possibility for the thief to block the remote control function by simply staying offline, thereby retaining an opportunity to break into the device.

b. Application-Level Security

At Apple's Worldwide Developer's Conference in San Francisco, June 2014, CEO Tim Cook announced many impressive business facts and numbers. Among them were that there are 1.2 million applications (apps) available on the iTunes App Store and 75 billion application-downloads. Presently, consumers rely heavily on the applications installed on their devices to aid in activities ranging from entertainment such as games, videos, and music to professional services such as banking, financial analysis, and health monitoring. There are currently 23 different application categories listed in the Apple App Store. [17] The complicated relationship between user behaviors and business opportunities in the smartphone market has created a gap where malicious acts can be carried out. Not until the recent information security breaches such as Edward Snowden, Target, and Heartbleed, did smartphone users start realizing the significance of information security.

The application-level security generalizes many security-related functions that smartphone applications can do. More specifically, the application-level security functions include data encryption/protection, authentication, application disablement/containment, VPN, and geo-fencing.[18] These functions all have their own unique role in defending smartphones against malicious attacks. For example, the disablement function can disable location tracking-related applications when users

---

[16] Donna Tapellini, "Smart Phone Thefts Rose to 3.1 Million Last Year, *Consumer Reports* Finds," *Consumer Reports*, May 28, 2014, http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.

[17] Apple Inc., "App Store Downloads on iTunes," accessed February 11, 2015, https://itunes.apple.com/us/genre/ios/id36?mt=8.

[18] Wheeler, "Smartphone Security."

conduct sensitive operations or disable smartphone sensors when users enter restricted areas. The geo-fencing feature can allow implementation of needed security settings based on the location of the smartphones. It is important to note that application-level security is critical during the application design and development phases. Every shortcoming in addressing all facets of application-level security concerns will result in potential product vulnerabilities and exploitation for an attacker.

In addition, application-level security can also be part of the emerging Mobile Application Management (MAM) capability, which gives the device owners or the administrators the ability to enforce application security policy and perform application classification.[19] There are two main MAM strategies: app containerization and app wrapping. Containerization is a term to describe the separation or division between the corporate and personal applications and data on the smartphone.[20] Wrapping means applying an additional management layer to an applications or a group of applications.[21] The app containerization demands intense coding and often results in negative impact on device performance and user experience by requiring users to switch in and out of "containers" between work and personal use.[22] In contrast, the app wrapping requires no coding and its perceived simplicity has helped its popularity to exceed that of the containerization approach. In 2013, ABI Research predicted the application wrapping adoption would grow at a 27% rate through 2018, whereas containerization will grow at a 23% rate in the mobile workspace management market.[23]

[19] Margaret Rouse, "Mobile Application Management (MAM)," TechTarget, June 2014, http://searchconsumerization.techtarget.com/definition/mobile-application-management.

[20] Ken Lienemann, "Containerization: Balancing BYOD for the Enterprise and You," *Wired*, June 24, 2014, http://insights.wired.com/profiles/blogs/containerization-balancing-byod-for-the-enterprise-and-you#axzz3RTOachqw.

[21] Margaret Rouse, "App Wrapping (Application Wrapping)," TechTarget, July 2012, http://searchconsumerization.techtarget.com/definition/app-wrapping-application-wrapping.

[22] Declan McNamara, "Balancing Corporate Security with User Experience," IBM, April 5, 2013, http://asmarterplanet.com/mobile-enterprise/blog/2013/04/balance-corporate-security.html; Stephen Skidmore, "App Wrapping Is a Form of Containerization," Apperian, April 16, 2014, http://www.apperian.com/app-wrapping-is-a-form-of-containerization/.

[23] ABI Research, "App Wrapping and Container Technologies to Drive Mobile Workspace Management Subscribers Past 60 Million by 2018," September 16, 2013, https://www.abiresearch.com/press/app-wrapping-and-container-technologies-to-drive-m/.

c. *Antivirus/Firewall*

Unlike the Apple iOS applications, which undergo extensive reviews before release to the public, many Android applications are insufficient in mobile security risk mitigations. Worst of all, there are malicious applications made available to the public, prompting the development of smartphone antivirus/firewall applications. What makes the mobile antivirus applications different from other mobile security applications is the performance requirements. Smartphone users expect mobile antivirus applications to be always-on, compared to the other security functions that only need to perform when specific actions require it.

Typically, the antivirus, antispam, virus scan, and firewall applications in personal computers and smartphones have the same objectives. However, due to the fundamental differences between personal computers and smartphone design in terms of power source, computing power, and operational system structure, the mobile antivirus application does not behave in the same way as it does in personal computers. For example, an antivirus application in the Apple iOS environment cannot automatically access and scan contents existing in the iOS or other applications due to the iPhone's "sandbox" practice, which is where applications are separated from the iOS and other applications by default. This means that if you want to scan an email attachment, you will need to manually send the attachment to the antivirus application first before conducting the virus scan.[24] Furthermore, the antivirus is just another application that rests above the smartphone OS instead of within it. To clarify, if the phone itself was "jailbroken," or "rooted," a form of device privilege control and escalation, the antivirus application is now vulnerable to the malware embedded in the OS instead of being able to protect the OS against it.[25]

---

[24] Eric Beehler, "How Mobile Antivirus Software Works and How to Know If You Need It," TechTarget, March 2014, http://searchconsumerization.techtarget.com/opinion/How-mobile-antivirus-software-works-and-how-to-know-if-you-need-it.

[25] Serge Malenkovich, "Rooting and Jailbreaking: What Can They Do, and How Do They Affect Security?," *Kaspersky Lab* (blog), May 31, 2013, http://blog.kaspersky.com/rooting-and-jailbreaking/.

2. Hardware-Based Smartphone Security (OEM)

In 2012, the National Institute of Standards and Technology (NIST) published the *Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)*, which pointed out: "Mobile devices are vulnerable to 'jailbreaking' and 'rooting,' which provided device owners with greater flexibility and control over the devices, but also bypasses important security features which may introduce new vulnerabilities." [26] Although common smartphone security solutions are software-based, some of these solutions have been proven inadequate and inefficient for meeting the higher security requirement demanded by government agencies and military units. [27] According to NIST's findings and guidelines, many mobile devices are not capable of providing strong security assurance because they lack hardware-based security solutions. The software-based solutions' easily mutable and manipulate-able nature is the cause of recent increases in hardware-based smartphone security investments and developments.[28]

The significance of the hardware-based solution is its immutability and reliability compared to its software-based counterpart.[29] Instead of protecting the smartphones at the outer layers (user and application), the hardware-based solution now provides protection to the inside layers (server, hardware, and OS). From various resources including the NIST's guidelines on mobile security, the National Security Agency's High Assurance Platform (HAP) initiative, and Trusted Computing Group's research and development, one can identify four trending hardware-based mobile security technologies: hypervisor (virtualization), Trusted Platform Module (Roots of Trust/RoTs), secure operating system, and secure SIM.

---

[26] Lily Chen, Joshua Franklin, and Andrew Regenscheid, *Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)* (Gaithersburg, MD: National Institute of Standards and Technology, October 2012), 1, http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf.

[27] Wheeler, "Smartphone Security"; Robinson, "Hardware-Based Mobile Security Market Heats Up."

[28] Robinson, "Hardware-Based Mobile Security Market Heats Up."

[29] Chen, Franklin, and Regenscheid, *Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)* (Gaithersburg, MD: National Institute of Standards and Technology, October 2012), 1.

a. *Hypervisor (Virtualization)*

A hypervisor is a manger or monitor for all running virtual machines (VMs) on a host computer system.[30] There are Type I bare-metal hypervisors and Type II hosted hypervisors. The fundamental difference between the two types is where the hypervisor is located in the computer architectures. Type II resides on top of the device OS such as Mac OS, Windows 8, and Linux, while Type I resides below the device OS.[31] Implementing a Type I hypervisor in smartphones requires more extensive hardware support, which imposes higher costs and requires more time for the smartphone manufacturers to develop new smartphone products. In contrast, although it is easier to install a Type II hypervisor on to devices, it is still difficult to do because the modern smartphone OS is either tightly controlled (Apple iOS) or heavily customized (Android).[32]

Strictly speaking, a hypervisor is considered a piece of software. However, since it is one of the OEM smartphone security solutions, we addressed this solution under the hardware-based smartphone security section. To most computer users, virtualization is just a way to run multiple operational systems on a single computer system. However, to government and business organizations, virtualization means more than just doing more with less—it is better security management and lower security risk. Part of the design requirements for a hypervisor is to mediate VM access to the host device's physical resources, provide isolation among VMs, and enable secure connections among VMs and to the external network.[33]

---

[30] Margaret Rouse, "Hypervisor," TechTarget, October 2006, http://searchservervirtualization.techtarget.com/definition/hypervisor.

[31] Bill Kleyman, "Hypervisor 101: Understanding the Virtualization Market," Data Center Knowledge, August 1, 2012, http://www.datacenterknowledge.com/archives/2012/08/01/hypervisor-101-a-look-hypervisor-market/.

[32] Kurt Marko, "3 Ways To Virtualize Mobile Devices—And Why You Should Do So," *InformationWeek*, July 2, 2013, http://www.darkreading.com/risk-management/3-ways-to-virtualize-mobile-devices----and-why-you-should-do-so/d/d-id/1110613?.

[33] Ramaswamy Chandramouli, *Security Recommendations for Hypervisor Deployment* (Gaithersburg, MD: National Institute of Standards and Technology, October 2014), http://csrc.nist.gov/publications/drafts/800-125a/sp800-125a_draft.pdf.

When the iPhone was first introduced in 2007, few could visualize the mobile virtualization on its 32-bit/412 MHz CPU and 128 MB RAM simply because of its limited computing power.[34] The recently released iPhone 6 features a 64-bit/1.4 GHz dual-core CPU and 1 GB RAM, which is potentially more powerful than some of the PCs on the market.[35] The recent increase in computing power in smartphones has made mobile virtualization possible, for a smartphone hypervisor allows a single device to have multiple virtual phones (VPs) that account for the dynamic mobile environment and separation of work and personal data. The U.S. Marine Corps' Trusted Handheld Platform effort is an example of achieving high-level security assurance and minimizing attack surfaces by operating an independently customized and trusted secure OS on a smartphone hypervisor.[36]

In addition, the virtualization has extended deeper into the hardware level, for the new type of hypervisor (Type 0) has already been developed and implemented. Figure 2 shows how different types of hypervisors reside with respect to the host hardware and OS and lists the average size of each type. The Type 0 hypervisor is the smallest in size and closest to the hardware component, which provides hackers a minimum attack surface and users a more stable and secure virtual operating environment.[37]

---

[34] EveryiPhone.com, "Apple iPhone (Original/1st Gen/EDGE) 4, 8, 16 GB Specs," accessed February 11, 2015, http://www.everymac.com/systems/apple/iphone/specs/apple-iphone-specs.html.

[35] EveryiPhone.com, "Apple iPhone 6 (GSM/North America/A1549) 16, 64, 128 GB Specs," accessed February 11, 2015, http://www.everymac.com/systems/apple/iphone/specs/apple-iphone-6-a1549-4.7-inch-gsm-north-america-specs.html.

[36] John McHale, "For Every Soldier, a Smartphone," Military Embedded Systems, October 9, 2013, http://mil-embedded.com/articles/for-every-soldier-smartphone/.

[37] Lynx Software Technologies, Inc., "The Rise of the Type Zero Hypervisor," accessed February 11, 2015, http://www.lynx.com/whitepaper/the-rise-of-the-type-zero-hypervisor/.
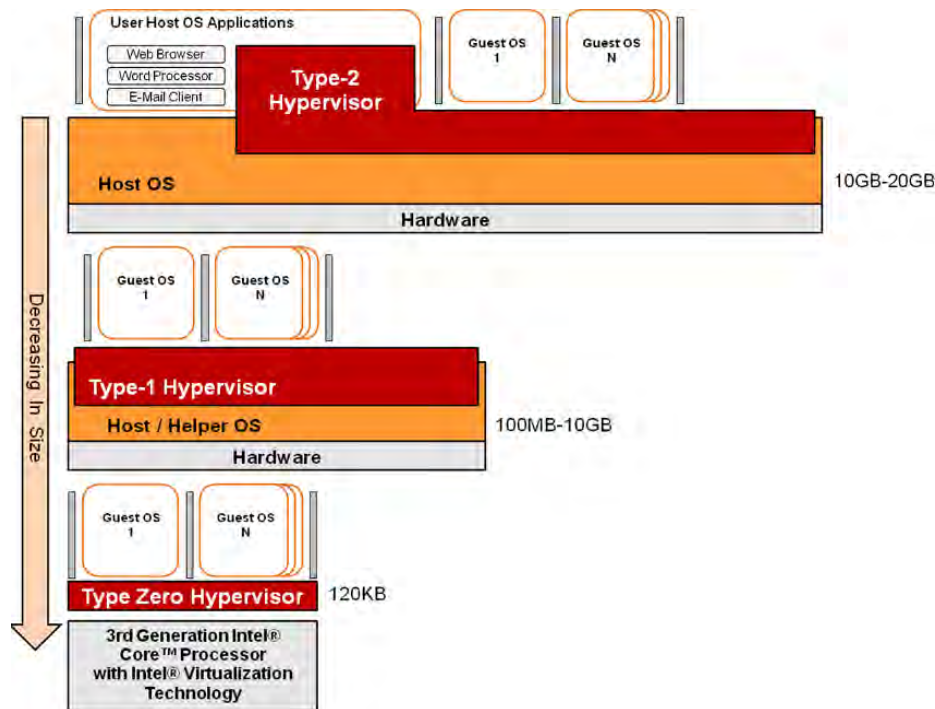
Figure 2.   Hypervisor Size Chart[38]

With support of the embedded architecture in the processor, the Type 0 hypervisor is able to perform memory and resource separation to create separate virtual environments.[39] The ability to perform physical separation is significant since it allows for complete domain isolation and application containerization, which are both critical in countering virtualization escape attacks. For example, the NSA's HAP uses Intel's hardware virtualization technology to protect execution space and memory to prevent resources in one domain from unauthorized access by hardware and software from another domain.[40]

The capability to form separate virtual smartphone domains and seamlessly switch from one virtual smartphone to another exists. Yet, there are several problems in adapting this practice, which ties deeply with users' habits and the blurred lines between

[38] Ibid.

[39] Ibid.

[40] National Security Agency, "NSA's First Trusted Computing Conference and Exposition," accessed February 12, 2015, https://www.nsa.gov/public_info/media_center/ia/video/orlando2010/transcript.html; "HIGH ASSURANCE PLATFORM® (HAP)," National Security Agency, accessed February 11, 2015, https://www.nsa.gov/ia/_files/hap_ds.pdf.

17

work and personal spaces. As Tal Klein, former Director of Technical Marketing for Citrix, pointed out:

> In the dual persona use case, IT is forcing end-users who don't have multiple personalities to adopt multiple personalities. This is not holistic and forces people to work in a different context because IT says so with no added benefit to the end-user. It is contrary to how we interact with our computing devices, especially phones and thus destined to fail.[41]

Allegorically, safety goggles cannot protect people's eyes if no one likes to wear them. In this case, the same applies to virtual safe smartphones: the organization cannot ensure smartphone security if no one likes to use the security measures due to cumbersomeness or performance degradation.

b.   *Trusted Platform Module (Roots of Trust, RoTs)*

The Trusted Platform Module (TPM) is a trusted computing technology developed and implemented by the Trusted Computing Group (TCG), a global industry standards group that includes members such as Intel, Microsoft, IBM, Dell, and Hewlett-Packard. TPM is a separate hardware component that integrates various computing devices including smartphones. First introduced in 2003, TPM drove the creation of the entire trusted computing ecosystem.[42] In light of the mobile computing expansion and the BYOD trend, the computer industry is eager to expand the trusted computing envelope over the smartphone domain.

The TPM, a small computer (microcontroller), is comprised of a secure cryptoprocessor, a protected memory, and a programmable input/output peripheral. It performs hardware encryption and safe information storage to create the "Trust

---

[41] Gunnar Berger, "Gartner Catalyst 2012: Is the Mobile Hypervisor the Right BYOD Approach?," Gartner Inc. (blog), August 7, 2012, http://blogs.gartner.com/gunnar-berger/gartner-catalyst-2012-is-the-mobile-hypervisor-the-right-byod-approach/.

[42] Trusted Computing Group, "Trusted Platform Module (TPM) Summary," accessed February 11, 2015, http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary; Mike Boyle, "Trusted Computing Standards Overview," National Security Agency, October 4, 2012, http://scap.nist.gov/events/2012/itsac/presentations/day2/4Oct_1145am_Boyle.pdf.

Boundary."[43] The environment enclosed within the trust boundary has led to the creation of the Roots of Trust (RoTs) concept. In NIST's *Guidelines on Hardware-rooted Security in Mobile Devices (Draft)*, the RoTs are defined as "security primitives composed of hardware, firmware, and/or software that provide a set of trusted, security-critical functions."[44] The RoTs are particularly instrumental to attestation.

Attestation (hardware authentication) is a mechanism for device integrity validation. It compares the device integrity measurements collected at different times to verify integrity or detect modification of the device.[45] Using the result from the attestation, the device can block unauthorized modifications or maliciously installed codes from executing until proper remediate actions or reinstatements are performed.[46] The attestation is done locally within the device or remotely on a network server to manage access control. This deep-level security function involves the following roots of trust:

- Root of Trust for Measurement (RTM): The RTM measures the device's integrity. The integrity measurement usually is an encrypted software image file or device configuration file.

- Root of Trust for Integrity (RTI): The RTI provides protected location where stores the integrity-sensitive data such as boot time measurement.

- Root of Trust for Reporting (RTR): The RTR performs identity and signature services on the integrity measurement data during the attestation process.

- Root of Trust for Confidentiality (RTC): The RTC provides protected location for storing confidential data such as encryption keys. Although both RTI and RTC try to protect the stored data, the most significant difference between the two is that RTI data can be shared but RTC data

---

[43] Thomas Hardjono and Greg Kazmierczak, *Overview of the TPM Key Management Standard* (Beaverton, OR: Trusted Computing Group), accessed February 11, 2015, https://www.trustedcomputinggroup.org/files/resource_files/ABEDDF95-1D09-3519-AD65431FC12992B4/Kazmierczak20Greg20-20TPM_Key_Management_KMS2008_v003.pdf.

[44] Chen, Franklin, and Regenscheid, *Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)* (Gaithersburg, MD: National Institute of Standards and Technology, October 2012), 1.

[45] Kathleen N. McGill, "Trusted Mobile Devices: Requirements for a Mobile Trusted Platform Module," *Johns Hopkins APL (Applied Physics Laboratory) Technical Digest* 32, no. 2 (2013): 545.

[46] National Security Agency, "NSA's First Trusted Computing Conference and Exposition."

cannot. Therefore, RTI and RTC require different access control interfaces.

- Root of Trust for Verification (RTV): The RTV verifies the integrity of the device and its software and date. This can be achieved by comparing the stored integrity measurements or matching the encryption keys.

Figure 3 shows typical RoTs interactions in the trusted computing attestation mechanism. First, the RTM requests the integrity measurements of the latest platform configurations and stores the information in the RTI. It is important to understand that the RTM does not actively perform the integrity measurement, but rather the host software conducts the measurements and sends them to the RTM.[47] Usually, the measurement process occurs during the boot cycle where RTM is provided with the most genuine information. During an attestation, a trusted computing application asks the RTR to deliver a signed integrity measurement report. The RTR then retrieves the integrity measurements stored in the RTI, signs the data with RTC encryption keys, and reports the data back to the trusted computing application for the attestation.[48]
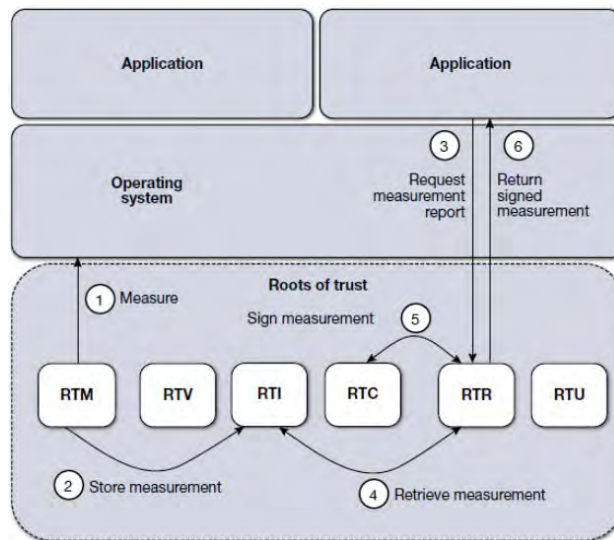
Figure 3.   Root of Trust Interactions for an Attestation[49]

[47] Raymond Ng, "Trusted Platform Module TPM Fundamental," Infineon Technologies, August 2008, http://www.cs.unh.edu/~it666/reading_list/Hardware/tpm_fundamentals.pdf.

[48] McGill, "Trusted Mobile Devices," 547.

[49] Ibid.

The significance of the TPM and RoT concept is to create a trusted flow (Measure, Verify, and Execute) in smartphones to ensure not only device integrity but also network integrity.[50] The establishment of the trusted flow within different smartphone security layers is the anchor of the overall security of the smartphone ecosystem. However, the TPM still has its own vulnerabilities to malicious attacks such as using physical objects to reset and bypass TPM chip security features, exploiting dynamic random access memory (DRAM) trace effects that allow the retrieval of contents stored in the DRAM without initiating TPM attestation process, and social engineering. One way to mitigate the TPM security risk is to eliminate unauthorized physical access to the TPM chip.[51]

c.   *Secure Operating System*

The importance of a well-designed and well-written secure operating system cannot be overstated. The operating system is where both software- and hardware-based solutions interact like a medicine and an organ do within our immune system. A secure operating system can dramatically reduce the dependence of the third-party security solutions and the overhead cost of the hardware security development. Based on a report dated April 2014 from Gamma Group, one of the most prominent surveillance companies in the world, the iPhone is still the most secure smartphone. It is critical to understand that a secure operating system does not guarantee a secure smartphone. The secure operating system is only part of smartphone security chain, a collaboration of secure software, hardware, and service.[52]

In the case of Apple iOS, one of its secure features is "sandboxing," which is a term to describe the mobile security approach of limiting or isolating the environments in

---

[50] Ibid.

[51] Philip Roman et al., "Trusted Platform Module," *ResearchedSolution* (blog), November 25, 2012, https://researchedsolution.wordpress.com/2013/09/14/trusted-platform-module/.

[52] Craig Timberg, "Why Surveillance Companies Hate the iPhone," *Washington Post*, August 11, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/08/11/why-surveillance-companies-hate-the-iphone/; Apple Inc., *iOS Security*, October 2014, https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

which only certain code can execute to prevent unauthorized interactions.[53] In the iOS security architecture, the encrypted file system has already been partitioned into its user and OS parts. This initial separation shields the system file and resources from users and all third-party applications. Furthermore, within the user partition, each third-party application is sandboxed. The default sandboxing is to restrict all third-party applications from accessing data stored in other applications or from modifying the device. The sandboxing practice, along with the application review process, has dramatically reduced the chance of malicious intrusion and infection in the iOS. To improve the end-user experience, Apple has developed its own mobile device management (MDM) feature into the latest iOS version 8.[54] However, the jailbreaking process can strip away the security and MDM features and leave the smartphone vulnerable to third-party malicious applications.

d. Secure SIM

At the 2013 Black Hat security conference, Karsten Nohl, a security researcher with Security Research Labs, demonstrated the ability to exploit mobile SIM's outdated encryption standard and grant access to the device's SMS (Short Message Service), location information, and voicemail numbers. With nearly seven billion SIM card users globally, the SIM is considered the most common mobile security token in the world.[55] Therefore, any SIM vulnerability is a gateway to large-scale mobile security breaches, let alone the potential to impact the trend toward mobile device–based payment transactions. The SIM is a device identification and authentication specification formalized to appropriately manage user/network authorization. Similar to TPM, the SIM is also a small computer and acts as a trusted bridge between devices and network providers. There are total of 14 different types of information stored in the SIM, and they all serve

---

[53] "About App Sandbox," Apple Inc., accessed February 12, 2015, https://developer.apple.com/library/mac/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html.

[54] Apple Inc., *iOS Security*.

[55] Security Research Labs, "Rooting SIM Cards," July 31, 2013, https://srlabs.de/rooting-sim-cards/.

different purposes in various applications related to mobile service.[56] It is important to understand that the SIM is a separate entity from smartphones and is highly accessible and transferable. Therefore, to implement SIM security is as difficult and complicated as it is in smartphone device security. However, for the purpose of this study, we consider SIM security as part of smartphone security and focus on the SIM security applications in smartphone usage.

In a typical case of SIM card authentication, when a subscriber wants to make a phone call, the mobile station (MS) establishes a connection with the network base station (BS) and then relays the International Mobile Subscriber Identity (IMSI) from the SIM to the BS, or more accurately, a temporary value representing the IMSI. After the BS recognizes the registered IMSI, it will send a random number (RAND) back to the SIM via the MS. After receiving the RAND, the SIM processes it with its encryption key and produces an output called a signed response (SRES). The SRES, an encrypted text, is then transmitted back to the BS via the MS and is verified by the network to determine the authenticity and identity of the user device and to authorize the user to place a call. As the cellular network and smartphone technologies continue to evolve, the SIM is no longer just a simple security token for placing a phone call. It can also be the security token for the WLAN (Wireless Local Area network), NFC (Near Field Communication), and RFID (Radio-Frequency Identification) services.

Although the detailed SIM card–based security protocols vary in the cellular network, WLAN, and NFC services, the SIM card plays the same role as a security element in the overall mobile security scheme. Being a secure element means the guarantee of the integrity of stored contents. There are various ways to increase SIM security, such as better encryption mechanisms and device- or network-based SMS antivirus/firewall. Users must realize the fact that mobile data safety is directly tied to

---

[56] eBay, "SIM Card Guide," June 9, 2014, http://www.ebay.com/gds/SIM-Card-Guide-/10000000177629426/g.html.

SIM safety. [57] The potential risks derived from the secure SIM may not be fully quantifiable, for the security applications in both public and military mobile services, such as transport, access control (passport), bank/finance, and mobile money, can all greatly benefit from secure SIMs.

No networked system, including the smartphone, is completely or totally secure. There is no silver bullet for securing a smartphone successfully—this requires the collaboration and combination of various security technologies and applications. After understanding how to secure smartphones in a technical context, it is time to examine the policy context where the technology and user connect to realize the goals of smartphone security.

D.   MOBILE DEVICE INCORPORATION

A comprehensive process is the cornerstone to a successful mobile device incorporation program, which creates an environment optimized for information sharing between employer and employee. [58] The proliferation of smartphones has dramatically changed the traditional boundaries between personal environs and workspaces, and in doing so has created pressing needs for mobile device management. Many organizations face the pressures and challenges to obtain the right balance between productivity and security. Recognizing the inevitable smartphone implementation and social penetration, numerous well-known organizations such as the U.S. Department of Defense, IBM, and BlackBerry Ltd., have issued publications regarding mobile device strategy, implementation, and usage. Surveying these key documents led to the identification of the essential ingredients for a successful mobile device incorporation process.

---

[57] Sridher (Sree) Swaminathan, *Mobile/NFC Security Fundamentals: Secure Elements 101* (Princeton Junction, NJ: Smart Card Alliance, March 28, 2013), http://www.smartcardalliance.org/resources/webinars/ Secure_Elements_101_FINAL3_032813.pdf; Security Research Labs, "Rooting SIM Cards"; Alex Savitsky, "Weak Link: How (Not) To Lose Everything Having Lost Your SIM-Card," *Kaspersky Lab* (blog), November 17, 2014, http://blog.kaspersky.com/make-your-sim-secure/.

[58] Apple Inc., "iPad in Business—Bring Your Own Device," accessed February 12, 2015, https://www.apple.com/ipad/business/it/byod.html.

Figure 4 shows the process of becoming a mobile organization involves four parts in a closed loop: strategy, policy, technology, and education.[59]

Figure 4.　　Mobile Device Incorporation Process[60]

Each part has its own unique purpose in the organization mobilization process, yet all are interconnected to form a continuous cycle able to adapt to the ever-evolving mobile computing technologies. Interestingly enough, the process itself shares similarities with the system engineering process.

1.　　Strategy

All plans should start with a sound strategy. The strategy is the core of the incorporation plan. It gives organizations the reasons why they do what they do. A good strategy acts like a cohesive agent that unites employer and employees as a whole and creates a uniform ideology across the entire organization. For example, the opening line of the U.S. DOD Mobile Device Strategy is its Mobility Vision statement:

> A highly mobile workforce equipped with secure access to information and computing power anywhere at anytime for greater mission effectiveness.[61]

---

[59] Chris Pepin, "BYOD at IBM," IBM, January 31, 2013, http://www.slideshare.net/chrispepin/ibm-connect-2013-byod-at-ibm.

[60] Ibid.

At IBM, the former chief information officer (CIO), Jeanette Horan, also gave the entire organization a concise goal statement for the IBM BYOD program:

> [It] really is about supporting employees in the way they want to work. They will find the most appropriate tool to get their job done. I want to make sure I can enable them to do that, but in a way that safeguards the integrity of our business.[62]

The statement sets the keel of the incorporation plan by defining the plan to serve as the fundamental guideline for future policy, technology, and education parts. In the strategy section, certain critical information should be identify and defined. Without properly identifying and defining the key information the mobile device incorporation plan is destined to fail, resulting in catastrophic security breaches. Table 1 lists the key information and considerations for planners during the initial strategy part in developing the incorporation plan.

Table 1.   Key Strategy Information[63]

	Key Information	Considerations
1	Vision	What mobile means for your organization Why mobile is important to your organization Where your organization will be five years from now
2	Goal	What mobile advantages your organization wants to obtain What mobile risks your organization wants to avoid
3	Organization Character	What type of organization is yours What your organizational culture is like
4	User Behavior	What mobile means for your employees Why mobile is important to your employees How mobile your employees are now

---

[61] United States Department of Defense, *Department of Defense Mobile Device Strategy (Version 2.0)* (Washington, DC: United States Department of Defense, May 2012), http://www.defense.gov/news/dodmobilitystrategy.pdf.

[62] Pepin, "BYOD at IBM."

[63] SAP SE, *Bring Your Own Device (BYOD) Policy Guidebook: Questions to Ask and Best Practices to Consider*, accessed February 12, 2015, http://www.emedialaw.com/files/2013/02/SAP-BYOD-Policy-Guidebook2.pdf; Richard Absalom, *Beyond BYOD : How Businesses Might COPE with Mobility* (London: Ovum Ltd.), accessed February 12, 2015, http://us.blackberry.com/content/dam/blackBerry/pdf/business/english/Beyond-BYOD-BlackBerry-Ovum.pdf.

In addition to creating a concise strategy statement, the organization needs to choose the most suitable strategic option for its mobile device incorporation. These options are: 1) BYOD—Bring Your Own Device, 2) COPE—Corporate Owned Personally Enabled, 3) CYOD—Choose Your Own Device, and 4) COBO—Corporate Owned Business Only. Each option has specific benefits and drawbacks, and will suit certain scenarios, and organizations, better than others will, as depicted in Table 2.[64]

Table 2.   Strategic Options[65]

	Option	Benefit	Drawback	Suited Organization
1	BYOD	High flexibility Positive employee experience Low cost*	High security risk Employee privacy violation Complex MDM/MAM	Organizations embrace mobility and value employee productivity and experience
2	COPE	Low security risk High cost	Limited choice Employee privacy violation	Organizations recognize mobility advantage but prioritize security over employee productivity and experience**
3	CYOD	Low security risk High cost	Limited choice Employee privacy violation	
4	COBO	Lowest security risk Low cost Simple MDM/MAM	Negative employee experience Low flexibility	Organizations demands complete security
*Be aware of false economy. Studies have shown that the same activities can cost up to five times more on a personal plan than on a business plan due to subsidizing and reimbursing.[66] **Organizations often use CYOD alongside COPE option.[67]				

2.   Policy

After creating a strategy statement and selecting the strategic option, the organization must establish a policy that enables the vision and goals within this strategy.

---

[64] Absalom, *Beyond BYOD.*

[65] Ibid.

[66] Ibid.

[67] Ibid.

The policy section, the most complex portion of the entire plan, contains key information-related considerations in need of evaluation, such as the incorporation model, device model, management solution, and security standard and baselines.[68] It is essential for the planners to establish a comprehensive but also well-orchestrated policy because this is the hub that grants the mobile device strategy the ability to successfully and smoothly permeate every level and corner of the organization. Constructing a sound policy is time-consuming and complicated, but it is required. The policy itself is the collaboration of multiple departments such as information technology, security, acquisition, human resources, finance, and legal.[69] Each department has unique demands and special concerns for mobile device incorporation.

Most importantly, the policy directly influences the employee's cognitive reactions and behaviors. The employee's negative cognitive feelings are the biggest resistance to a successful mobile organization. A research commissioned by Raytheon revealed that 56% of survey respondents said that employee resistance is the biggest barrier to an effective mobile strategy.[70] Thus, planners must always consider user experience during the policy-drafting section. Table 3 provides the planners with the key guidance needed to construct the mobile device incorporation policy.

---

[68] Absalom, *Beyond BYOD*; Murugiah Souppaya and Karen Scarfone, *Guidelines for Managing and Securing Mobile Devices in the Enterprise Revision 1* (Gaithersburg, MD: National Institute of Standards and Technology, June 2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf; United States Department of Defense, *DOD Commercial Mobile Device Implementation Plan* (Washington, DC: United States Department of Defense, February 15, 2013), http://www.defense.gov/news/dodcMdimplementationplan.pdf.

[69] Pepin, "BYOD at IBM"; SAP SE, *Bring Your Own Device (BYOD) Policy Guidebook*.

[70] Ponemon Institute, LLC., *Security in the New Mobile Ecosystem*.

Table 3.   Key Policy Guidance[71]

	Department	Guidance
1	Information Technology	Establish secure corporate mobile infrastructures (networks access control, secure VPN, and antivirus/firewall) Establish MDM/MAM governance structure (include device loss/stolen response actions) Establish mobile device security updates/support/scan/monitor procedure
2	Security	Establish mobile device security certification process and security baseline Establish mobile device usage security protocols and regulations Establish data classification protocols and regulations
3	Acquisition	Establish a list of approved mobile devices Establish mobile device logistics and support procedure with vendors Establish fair contract between mobile network providers, mobile device vendors, and organization
4	Human Resources	Establish mobile device security training program (including incoming and exiting employees) Establish mobile device user classification protocols and regulations Establish mobile device security violation protocols and regulations
5	Finance	Establish mobile device usage charges and refund conditions Establish budget for mobile device incorporation plan
6	Legal	Establish mobile device terms and conditions that comply with regional privacy and data protection laws and regulations. Establish mobile device user agreements and consent with organization

3.   Technology

Without the appropriate technological support structure, the policy cannot be successfully implemented. Based on the chosen strategic option and first policy iteration, organizations need to identify suitable technologies to be implemented in the incorporation plan. Most of the popular technologies identified earlier in the smartphone security section will be implemented throughout multiple mobile device security aspects such as mobile device management (MDM), mobile application management (MAM), and network access control (NAC).

---

[71] SAP SE, *Bring Your Own Device (BYOD) Policy Guidebook*; Absalom, *Beyond BYOD*; United States Department of Defense, "DOD Commercial Mobile Device Implementation Plan"; Souppaya and Scarfone, *Guidelines for Managing and Securing Mobile Devices.*

Often times the policy and the current technological support do not match up, which creates increased opportunities for security breaches and potential for high consequential damages. The objectives of a pilot program are to examine the policy for completeness, identify defects, obtain user feedback, and make further corrections and improvements.[72] The importance of the pilot program cannot be understated, for prior to official rollout of the mobile device incorporation plan, the organization must form the least risky pilot group comprised of employees from various departments and levels to test the policy.[73]

4. Training

The artifacts of the first three sections in the mobile device incorporation process, strategy (Brain), policy (Nerve), and technology (Muscle), lead to the development of the final section, training (Practice). Training is a process to familiarize and master a particular skill or type of behavior through constant practice and improvement. The purposes of mobile device incorporation training is to help an organization's members understand mobile threats and vulnerabilities, to establish trusted mobile device user behaviors, to build a culture of security, and ultimately create a secure mobile enterprise.[74]

Mobile device incorporation planners need to be aware that the mobile device incorporation process is dynamic and continuous in nature. All parts in the process are interactive, interdependent, and interrelated. As a chain is only as good as the weakest link, a plan is only as good as the weakest part. Insufficient understanding of the domain results in an inadequate strategy, which causes the development of a poor policy, which leads to the acquisition of inadequate technology, which provides for insufficient training. To avoid this chain reaction of failure, it is critical to treat mobile device

---

[72] United States Department of Defense, *Department of Defense Mobile Device Strategy*; United States Department of Defense, *DOD Commercial Mobile Device Implementation Plan*.

[73] Symantec Corporation, "Infographic: Creating a Successful BYOD Policy," September 15, 2014, http://www.slideshare.net/symantec/infographic-39117177; SAP SE, *Bring Your Own Device (BYOD) Policy Guidebook*.

[74] Pepin, "BYOD at IBM."

incorporation as a complex system and to utilize the system engineering approach to ensure a success.

In the next chapter, we use the system engineering approach to unveil the most suitable technology, part of four key ingredients to successful smartphone incorporation, to the Taiwan navy. The system engineering approach examines feasible solutions based on the Taiwan navy's current problems, challenges, and needs regarding smartphone incorporation. Ultimately, the outcome of the next chapter will serve as a recommended building block to anchor the Taiwan navy's uncertain thoughts about leveraging and incorporating smartphones into its force structure.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SYSTEM ENGINEERING APPROACH

With more than 100 ships and 40,000 personnel, the Taiwan navy is certainly a large and complex organization that can be viewed as a system. The International Council on System Engineering (INCOSE) system engineering handbook defines the term *system* as:

> A combination of interacting elements organized to achieve one or more stated purposes.
>
> An integrated set of elements, subsystems, or assemblies that accomplish a defined objective. These elements include products (hardware, software, firmware), processes, people, information, techniques, facilities, services, and other support elements.[75]

The Taiwan navy perfectly fits the definition of a system, as do smartphone devices. Many will argue that one is an organization and the other is a device, and that they are very different in many levels. However, from a system engineer's perspective, each of them is comprised of interacting elements to achieve certain goals, which resembles the essence of a system.

In an environment where one system needs to integrate with another system, there are challenges, including short technology life-cycles, evolving technology, greater utilization of COTS, and dwindling resources.[76] Often when system development or integration is poorly managed, the results are low system effectiveness and high total cost.[77] In order to achieve the right balance between effectiveness and cost, the Taiwan navy needs to use a system engineering approach to incorporate smartphone devices into its force structure.

---

[75] Cecilia Haskins, *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, 3.2.2 ed. (San Diego, CA: International Council on Systems Engineering, 2011), 5.

[76] Benjamin S. Blanchard, *System Engineering Management*, 4th ed. (Blacksburg, VA: John Wiley & Sons, 2008), 9.

[77] Ibid, 12–13.

A.   DEFINITION OF SYSTEM ENGINEERING

The INCOSE defines the term *system engineering* as

> an interdisciplinary approach and means to enable the realization of successful system. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal. SE considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs.[78]

The U.S. Department of Defense (DOD) defines *system engineering* as

> An approach to translate approved operational needs and requirements into operationally suitable blocks of systems. The approach shall consist of a top-down, iterative process of requirements analysis, functional analysis and allocation, design synthesis and verification, and system analysis and control. Systems engineering shall permeate design, manufacturing, test and evaluation, and support of the product. Systems engineering principles shall influence the balance between performance, risk, cost, and schedule.[79]

Leveraging a system and system engineering approach in the Taiwan navy is the key to successful smartphone incorporation. It is important for the Taiwan navy to see itself as not only an organization, but as a system, and that a smartphone is not only an electronic device, but also a system that needs proper management to accomplish the desired objectives. System engineering is the appropriate approach to enable the realization of a successful system and the perfect balance between performance, risk, cost, and schedule.[80]

B.   APPROACH FRAMEWORK—VEE MODEL

The Vee model is used to describe the life cycle of a system engineering process. It consists of two sides. The left side of the Vee represents the top-down evolution of user requirements into product design. The right side represents the bottom-up process of

---

[78] Haskins, *Systems Engineering Handbook,* 6.

[79] Blanchard, *System Engineering Management,* 17.

[80] Haskins, *Systems Engineering Handbook,* 7; Blanchard, *System Engineering Management,* 17.

system integration and verification.[81] Furthermore, there are two axes associated with the Vee model: vertical time axis and horizontal maturity axis.[82] The vertical axis represents the in-progress management activities that exist in both the left and right side of the Vee model. The horizontal axis represents the solution evaluation activities that connect both sides.
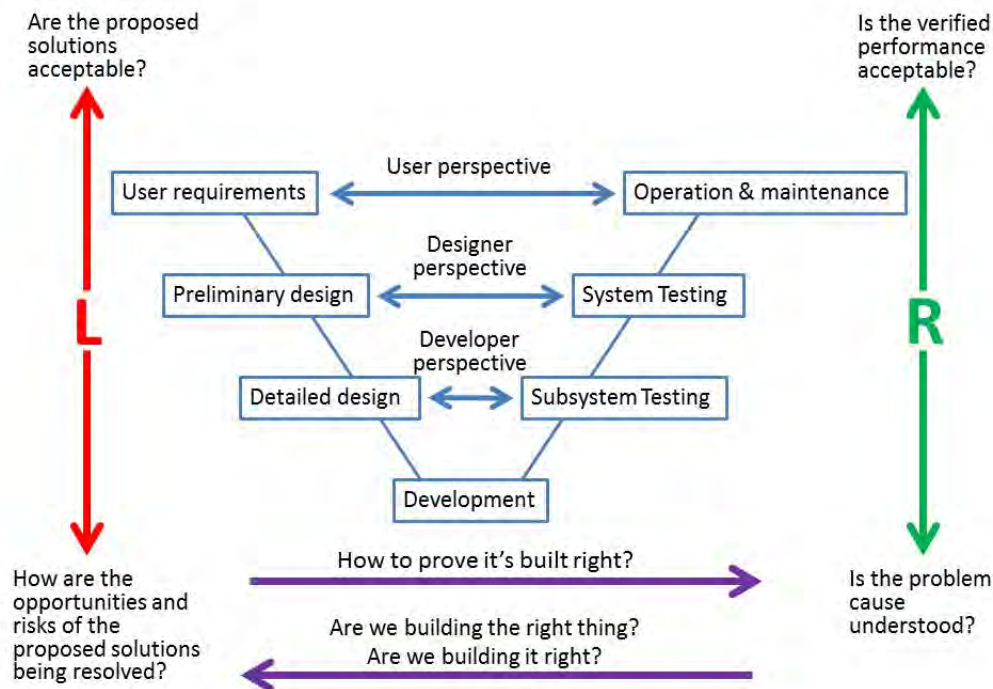
Figure 5.   Vee Model[83]

Figure 5 perfectly illustrates the interrelation between each of the seven stages within the Vee model. It is important to understand that the Vee model is not unidirectional but multidirectional. This multidirectional characteristic allows the system development to have a clear path in creating a mature product, while providing a feedback channel to validate and verify the product.

---

[81] Blanchard, *System Engineering Management*, 19.

[82] Haskins, *Systems Engineering Handbook,* 27–32.

[83] Blanchard, *System Engineering Management,* 29; Haskins, *Systems Engineering Handbook,* 28, 31.

The *Defense Acquisition Guidebook* (DAG) published by the U.S. DOD also provides insights about the Vee model. DAG's Vee model is supported by 16 processes (eight technical processes, and eight technical management processes), as listed in Figure 6.[84]
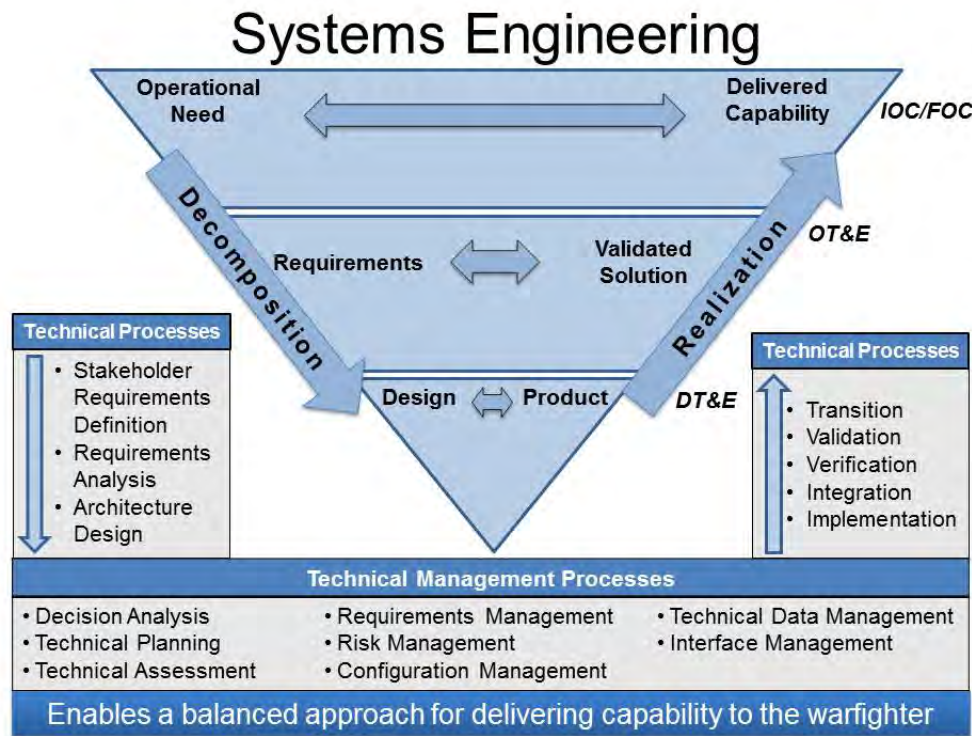
Figure 6.   DAG Vee Model[85]

In the DAG, these technical processes, along with the Vee model, provide a structured approach to increasing the likelihood that the capability being developed balances mission performance with cost, schedule, risk, and design constraints. Ultimately, the purpose of a system engineering approach is to provide a framework that allows organizations to efficiently and effectively deliver a capability or product to satisfy a validated operational need while reducing technical and programmatic risk.[86]

---

[84] United States Department of Defense, *Defense Acquisition Guidebook* (Washington, DC: United States Department of Defense, 2013), 160–62.

[85] Ibid, 162.

[86] Ibid., 160–62.

1. Modified Vee Model for the Taiwan Navy

Considering the conservative culture, limited resources, operational environment, and threat scenario, the Taiwan navy should scale the application and use of the Vee model to reflect the unique needs of the desired program or system being developed.[87] For the purpose of this analysis, first and foremost, we decided to replace the design and develop stages with just the COTS selection stage. This decision was made for numerous reasons, such as lower cost, faster and simpler development life-cycle, sufficient logistics and support, and better system maturity and reliability. Therefore, the Vee model for the Taiwan navy shown in Figure 7 is comprised of two main perspectives: the Taiwan navy and a COTS solution.

In the Taiwan navy perspective, we define and analyze the stakeholder requirements to determine the desired functionalities and capabilities required to support naval operations. In the COTS solution perspective, we exam and compare the Android, iOS, and BlackBerry system to determine the best solution for the Taiwan navy.
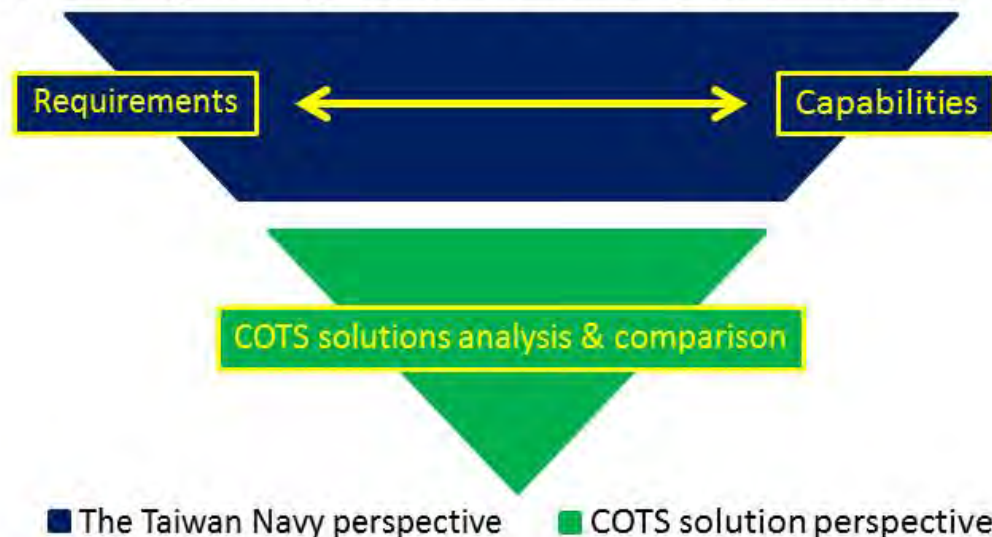
Figure 7.   The Taiwan Navy Vee Model

---

[87] Ibid, 162.

2. The Taiwan Navy Case (Problems, Challenges, and Needs)

The Taiwan navy has always emphasized the significance of information security to preserve operational advantages over the People's Liberation Army's (PLA) Navy. The PLA's persistent espionage efforts towards Taiwan have resulted in several incidents that forced the Taiwan navy to continue to increase its information security measures. Although none of the Chinese espionage cases resulted in direct access to information, the growing use of mobile devices, along with sophisticated PLA cyberattack attempts, may result in a successful attack that gains direct access in the near future.[88]

a. Problem

The criticality of information security has made the Taiwan navy's Information Technology (IT) structures and regulations cumbersome. This has slowed the Taiwan navy's information flow and has crippled the information technology incorporation process, particularly for mobile devices. The crippled process results in ineffective plans and consequently not only undermines operational and administrative productivity but also poses a greater risk to security and maneuverability in information warfare.

b. Challenge

The challenge to the Taiwan navy is how to balance productivity and security in the information domain, while incorporating the existing mobile ecosystem. The dilemma of productivity and security has long been a challenge for many organizations in the information age. Raytheon research found that "52 percent of survey respondents say security practices on mobile devices have been sacrificed in order to improve employee productivity."[89] The struggle of solving this dilemma has either placed organizations at a great security risk or dramatically decreased the overall improvement to productivity offered by the device adoption. In recent years, the introduction of mobile device security measures such as trusted computing, virtualization, and application management has mitigated some of this dilemma.

---

[88] Peter Mattis, "China's Espionage against Taiwan (Part I): Analysis of Recent Operation," *China Brief* 14, no. 21 (November 7, 2014): 6.

[89] Ponemon Institute, LLC., *Security in the New Mobile Ecosystem*.

c.   *Need*

Ultimately, the Taiwan navy needs a comprehensive smartphone incorporation plan to address the dilemma between productivity and security. Since the Taiwan navy has always maintained high information security demands, we decided to first identify the most secure smartphone system and use it as the starting point for a successful smartphone incorporation plan.

C.   TAIWAN NAVY PERSPECTIVE

During my three years of experience in the Taiwan navy as a junior officer onboard a surface ship, I had the opportunity to closely observe the information productivity and security issues encountered in both maritime and ashore scenarios. Often times, surface ships have only two phone lines and access to the Taiwan navy intranet when in port. To the officers onboard, these limited resources cannot satisfy their intense needs for unobstructed communications and up-to-date information, a situation often resulting in the use of personal mobile phones to make work-related calls or calls to colleagues in order to find out information not available on the ship's intranet. To save personal expenses, many service members in the Taiwan navy have an extra Asia Pacific Telecommobile phone dedicated to work-related communications using its free in-net calls policy to limit their out-of-pocket cost.[90] The cumbersome information security regulations not only create inefficient communications but also keep surface ships from leveraging the computing technologies. In 2013, there still were some computers onboard my ship running the Intel Pentium 4 processor.

The purpose of pointing out the constraints of the current Taiwan navy information policy is to introduce the advantages and potential of the mobile computing ecosystem, especially smartphone technologies and their related applications. These smartphones and their related applications provide the Taiwan navy a feasible solution to the dilemma of productivity and security.

---

[90] Asia Pacific Telecom, "Introduction to APT (Asia Pacific Telecom)," accessed February 24, 2015, http://ir.aptg.com.tw/en/APTIntroduction.htm.

1. System Requirements

For an information system to operate in a military organization or environment, security is always the top priority in system requirements. There is no exception regarding smartphone incorporation in the Taiwan navy. The smartphone must satisfy the widely used information system security criteria: confidentiality, integrity, and availability, also known as the CIA triad. In the most recent United States Committee on National Security System (CNSS) Instruction 4009, released in April 2010, CNSS defines CIA as:

- Confidentiality: the property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.
- Integrity: the property whereby an entity has not been modified in an unauthorized manner.
- Availability: the property of being accessible and usable upon demand by an authorized entity.

Each criterion generates various system requirements for the smartphone such as encryption and authentication for confidentiality, file permission and user access control for integrity, and backup and recovery for availability.

To benefit from smartphone incorporation, the Taiwan navy needs more than just a secure information system. It needs a secure and productive system. Other than meeting security requirements, a productive system also needs to meet usability requirements to become appealing and accepted to all of the stakeholders. The International Organization for Standardization (ISO) defined the term usability in ISO 9241–11, published in 1998, as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."[91] An information system with high security but low usability is often cumbersome and frustrating, eventually leading users to abandon the device or search for workarounds.[92]

---

[91] International Organization for Standardization. *Ergonomic requirements for office work with visual display terminals (VDTs)—Part 11: Guidance on usability* (Genève, Switzerland: ISO, 1998), 2.

[92] Skidmore, "App Wrapping."

To make the system requirements more comprehensible to the stakeholders, we decided to present the requirements in the form of system capabilities. Based on security and usability requirements, we developed 15 suggested smartphone capabilities for the stakeholders in the Taiwan navy, as depicted in Table 4. Each capability is associated with a letter to show the corresponding requirement it aims to meet.

Table 4.   System Capabilities Chart

C: Confidentiality I: Integrity A: Availability U: Usability			
	System Capabilities	**S**	**P**
1	Safe, secured, and encrypted communication channels	C,I	
2	Safe, secure, and encrypted storages	C,I	
3	User and device identification, authentication, and attestation	C	
4	Antivirus and firewall	I	
5	Mobile management (device and application)	I	
6	Privacy protection (secure and anonymous web browsing)	C	
7	Remote controls (lock, wipe, disable and recovery)	C,A	
8	Self-diagnose and warning capability	I	
9	Geo-fencing (location-based security service)	A	U
10	Cost-efficient communication channels		U
11	Low unit cost		U
12	Powerful, practical, and popular designs and functionalities		U
13	Sufficient and easy logistics and supports		U
14	Entertainment and media (audio, photo, video, and game)		U
15	Connectivity to the Taiwan navy intranet		U
S is security and P is productivity			

2.   Stakeholder Interests

A stakeholder is defined as "a party that has an interest in an enterprise or project."[93] From our observation, and considering the context of smartphone use in the Taiwan navy, there are two "camps" of stakeholders distinguished by their respective understanding of the relationship between smartphones and information. One is conservative, and the other is adoptive. For the most part, shown in Table 5, the two

---

[93] Investopedia, "Stakeholder," accessed February 24, 2015, http://www.investopedia.com/terms/s/stakeholder.asp.

groups understand and agree upon the importance of both smartphone security and productivity requirements except for the entertainment and media capability. The conservative stakeholder is concerned that the misuse of the capability may lead to information security incidents, such as classified information leakage and inappropriate information on social media that inevitably results in negativity in the press and damage to the image of the Taiwan navy. On the other hand, the adoptive stakeholder sees the entertainment and media capability as an opportunity, or a gateway, to the empowerment and reinvention of the Taiwan navy in the information age. Both groups show low interest to the Taiwan navy intranet connectivity capability simply because such connectivity defeats the purpose of creating a physically separated military network.

Table 5.   Stakeholder Interests Chart

		High ■ Low	I	II
	System Capabilities		**I**	**II**
1	Safe, secured, and encrypted communication channels		H	H
2	Safe, secure, and encrypted storages		H	H
3	User and device identification, authentication, and attestation		H	H
4	Antivirus and firewall		H	H
5	Mobile management (device and application)		H	H
6	Privacy protection (secure and anonymous web browsing)		H	H
7	Remote controls (lock, wipe, disable, and recovery)		H	H
8	Self-diagnose and warning capability		H	H
9	Geo-fencing (location-based security service)		H	H
10	Cost-efficient communication channels		H	H
11	Low unit cost		H	H
12	Powerful, practical, and popular designs and functionalities		H	H
13	Sufficient and easy logistics and supports		H	H
14	Entertainment and media (audio, photo, video, and game)		L	H
15	Connectivity to the Taiwan navy intranet		L	L
I is the conservative stakeholder and II is the adoptive stakeholder				

3.   System Feasibility Analysis

Ultimately, the Taiwan navy is searching for a trusted system that has most of the capabilities in Table 4. We only considered the COTS solution because it allows faster

procurement, shorter time to deployment, lower overall life-cycle cost, and less technical and financial risk compared to a custom developed or build-your-own approach. There are two considered approaches: a single COTS system and a combination of COTS systems and applications. A single COTS system approach is referring to the so-called ultra-secure smartphone, such as the Black smartphone from Boeing, the Blackphone from Silent Circle, the CryptoPhone from GSMK, and the Privacy Phone from FreedomPop.[94] These smartphones were developed in light of increasing violations of customer privacy, awareness of government surveillance, and proliferation of spyware. Although these smartphones have started attracting attention in the smartphone market, most of them come with only limited proprietary applications pre-installed and have not yet established sufficient logistic and support infrastructure. Other pitfalls include being only Android-based, which limit user's choices, and that their "ultra-secure calling and texting" only means applying encrypted voice over IP (VoIP) service over a cellular network, which requires an extra subscription fee.[95]

Based on the information about these ultra-secure smartphones, Blackphone is our choice to represent the first approach because it has more specific and promising information available. It is selling for US$629 (plus shipping and any local taxes or duties for the destination address) and comes with a one-year subscription to its encrypted calling and texting, encrypted web browsing, and secure cloud backup services.[96] The Blackphone's customized Android supports all of the languages a regular Android does; however, Blackphone-specific applications do not support Chinese.[97]

---

[94] Boeing, "Boeing Black Smartphone," accessed April 10, 2015, http://www.boeing.com/defense/boeing-black/index.page; Blackphone, "Welcome to Blackphone," accessed April 10, 2015, https://blackphone.ch/; ESD America Inc., "ESD CryptoPhone," accessed April 10, 2015, http://esdcryptophone.com/; FreedomPop, "Privacy Phone," accessed April 10, 2015, https://www.freedompop.com/theprivacyphone.

[95] Jill Scharr, "Blackphone vs. FreedomPop's Privacy Phone: Security Showdown," Tom's Guide, March 7, 2014, http://www.tomsguide.com/us/blackphone-vs-freedompop-privacy-phone,news-18427.html.

[96] Blackphone, "Blackphone," accessed February 25, 2015, https://blackphone.ch/phone/.

[97] Blackphone, "What Languages Does Blackphone Support?," August 2, 2014, https://support.blackphone.ch/customer/portal/articles/1565177.

The second approach, a combination of COTS systems and applications, is referring to regular smartphones with third-party applications. Although the regular smartphones are designed for the general public, it does not mean that they are not secure. In fact, the increasing public awareness and emphasis on mobile security have caused major smartphone manufacturers to improve and develop more secure smartphones. Apart from this, with the help of third-party applications, regular smartphones can fill the gaps that ultra-secure smartphones cannot. Ultimately, depicted in Table 6, the second approach has an edge over the first approach by providing the Taiwan navy with logistics and support services that are already well established, functionalities that are more versatile, and more choices for secure and efficient communication.

Table 6.   System Feasibility Chart

■ High feasibility ■ Low feasibility		
System Capabilities	**I**	**II**[*]
1 Safe, secured, and encrypted communication channels	H	H
2 Safe, secure, and encrypted storages	H	H
3 User and device identification, authentication, and attestation	H	H
4 Antivirus and firewall	H	H
5 Mobile Management (device and application)	H	H
6 Privacy Protection (secure and anonymous web browsing)	H	H
7 Remote controls (lock, wipe, disable, and recovery)	H	H
8 Self-diagnose and warning capability	H	H
9 Geo-fencing (location-based security service)	H	H
10 Cost-efficient communication channels	L	H
11 Low unit cost	H	H
12 Powerful, practical, and popular designs and functionalities	L	H
13 Sufficient and easy logistics and supports	L	H
14 Entertainment and media (audio, photo, video, and game)	H	H
15 Connectivity to the Taiwan navy intranet	L	L
I is the single COTS system and II is the combination of COTS systems and applications		
*Most feasible approach		

4. System Operational Requirements

Our research is to provide the Taiwan navy with a viable smartphone incorporation option, not equipment certified for a combat environment. Smartphone devices may serve as a tool that helps increase the Taiwan navy's information access and productivity while maintaining organizational security. Therefore, the operational requirements for the smartphone system used by this thesis as a basis for the Taiwan navy's case are the same as those for regular consumer uses.

D. SOLUTION PERSPECTIVE

Through previous system requirement description and feasibility analysis, we recommend the Taiwan navy use the second option, a combination of COTS systems and applications. This option has lower technological risk and overall cost, higher system maturity and usability, and better supply and logistic support. To limit the endless possibility of different COTS systems and applications combinations, the solutions we proposed are limited to one OEM operating system including its built-in applications and two third-party applications. Based on Taiwan's mobile market share and its navy's security concerns, four OEM options are chosen: 1) Samsung Knox Android, 2) HTCpro Android, 3) Apple iOS, and 4) BlackBerry OS. We first analyze the four OEM options and then choose the third-party applications according to their strengths and weaknesses.

1. OEM Option Analysis

All four major smartphone manufacturers, Samsung, HTC, Apple, and BlackBerry, advertise their operating system as the best for enterprise mobility. BlackBerry has long been known for its leading role in mobile security development—it also became famous for being President Obama's smartphone. Some Samsung and Apple products have received the approval from the Defense Information Systems Agency (DISA) for U.S. DOD use.[98] HTC has partnered with IBM to address the needs of a corporate IT department to deploy appropriate mobile devices for secure enterprise

---

[98] Defense Information Systems Agency, "Secure Unclassified Mobile Devices and Wireless Services," accessed February 27, 2015, http://www.disa.mil/Enterprise-Services/Mobility/Devices-and-Wireless-Services.

mobility.[99] In order to conduct a comparative analysis of all four options, we referenced the system capabilities chart depicted in Table 6 to identify three key functional areas and constructed a functionality chart (Figure 8). The key functional areas are security, management, and productivity. The first area, security, has always been the key concern for smartphones that operate in a military organization. The second area, management, is the key to optimize smartphone security, and productivity, the third key area, is the premise upon which adoption of smartphones is based.
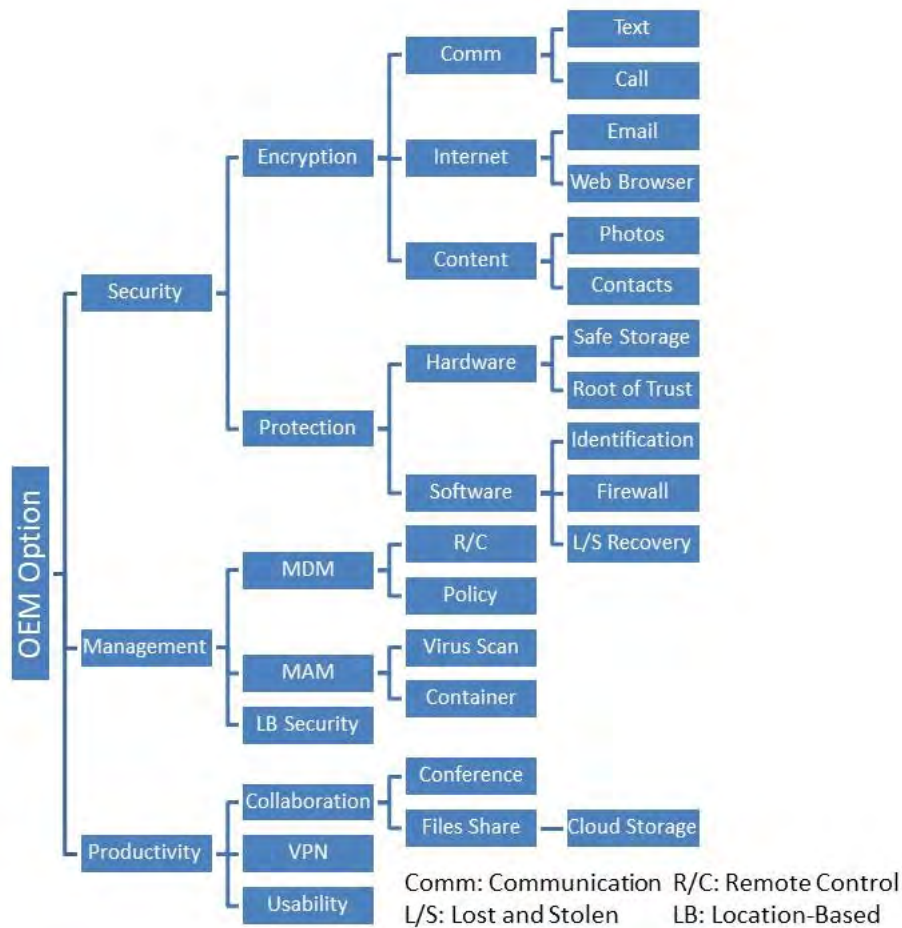
Figure 8.   Functionality Chart

[99] HTC Corporation, "HTCpro Partners," accessed February 27, 2015, http://www.htcpro.com/partners.

### a.	*Samsung Knox Android*

Samsung Knox employs an Android OS designed from the ground up with security and management enhancements. Its three security aspects, platform security, application security, and mobile device management, provide the Knox with a strong defense against malicious attacks. For U.S. government and DOD installations, Knox also provides attestation, supports smartcard/common access card (CAC) applications, and obtains certification and validation from NIST and DISA.[100] Table 7 summarizes the features and functionality in Samsung Knox and its related service.

Table 7.	Samsung Knox[101]

Features and Functionality		
Security	1	Customizable Secure Boot
	2	TrustZone-based Integrity Measurement Architecture (TIMA)—Linux kernel protection
	3	Security Enhancements for Android
	4	ARM TrustZone hardware[102]—Trusted computing/root of trust
	5	On-device Data Encryption (256-bit AES cipher algorithm)
	6	Internal SD card
	7	Smartcard/CAC support
	8	Two-factor biometric authentication
	9	Samsung Knox Apps store—Apps review
Management	1	Application containers
	2	Cloud-based MDM capability—VPN and Wi-Fi provisioning
	3	MDM IT policies enforcement*
	4	Single sign-on
	5	Device location and status tracking
	6	Remote lock, wipe, and passcode reset
	7	User activity report

---

[100] Samsung Electronics, *An Overview of Samsung Knox* (white paper) (Suwon-si, Korea: Samsung, June 2013), http://www.samsung.com/global/business/business-images/resource/white-paper/2014/02/Samsung_KNOX_whitepaper_June-0-0.pdf.

[101] Samsung Electronics, *An Overview of Samsung Knox*; Samsung Electronics, "Samsung Knox: Business Protection. Personal Privacy. One Device," accessed February 28, 2015, http://www.samsung.com/us/business/samsung-for-enterprise/downloads/KnoxBrochureSTA05_14.pdf; Samsung Electronics, "Knox Workspace—Technical Details," accessed February 28, 2015, https://www.samsungknox.com/en/products/knox-workspace/technical.

[102] ARM, "TrustZone," accessed February 28, 2015, http://www.arm.com/products/processors/technologies/trustzone/index.php.

Productivity	1	VPN (per-app feature)
	2	Samsung Knox Apps[103]—secure email, planner, contacts, camera and gallery, and browser, file & notes.
	3	Samsung Knox Apps store[104]—conference call, notes, files share, cloud storage, communication, print, etc.
*May vary by MDM partners		

The Samsung Knox Android does not have additional mobile call/text message encryption mechanisms or built-in antivirus/firewall functions factory-installed within the OS. Unlike the Apple iOS, Knox needs third-party services to provide cloud storage and conference call functionalities. These functional shortcomings can be easily remediated by third-party applications. The analysis and research also reveal that the Knox OS and factory-installed applications cannot realize the location-based security feature. It needs additional location monitoring and tracking infrastructure.[105]

We color-coded the functionality chart to provide a more comprehensive picture of the OEM option analysis. The color codes are green (strong), blue (moderate), and red (weak). The gradient color scheme represents the third-party applications improvement. In the Samsung Knox android option that depicted in Figure 9, we decided to use the Avast Mobile Security & Antivirus and GoToMeeting applications to improve its antivirus/firewall and conference call functionality.[106]

---

[103] Samsung Electronics, "Knox Workspace—Powerful Apps," accessed February 28, 2015, https://www.samsungknox.com/en/products/knox-workspace/features/powerful-apps#Camera-and-Gallery.

[104] Samsung Electronics, "Samsung Knox Apps," accessed February 28, 2015, https://www.samsungKnox.com/en/products/Knox-workspace/features/apps.

[105] AirPatrol Corporation, "ZoneDefense Location-Based Mobile Security Platform," accessed February 28, 2015, http://airpatrolcorp.com/products/zonedefense/#zd.

[106] Google Play, "Mobile Security & Antivirus—AVAST Software," accessed February 28, 2015, https://play.google.com/store/apps/details?id=com.avast.android.mobilesecurity&hl=en; Google Play, "GoToMeeting—Citrix," accessed February 28, 2015, https://play.google.com/store/apps/details?id=com.citrixonline.android.gotomeeting&hl=en.
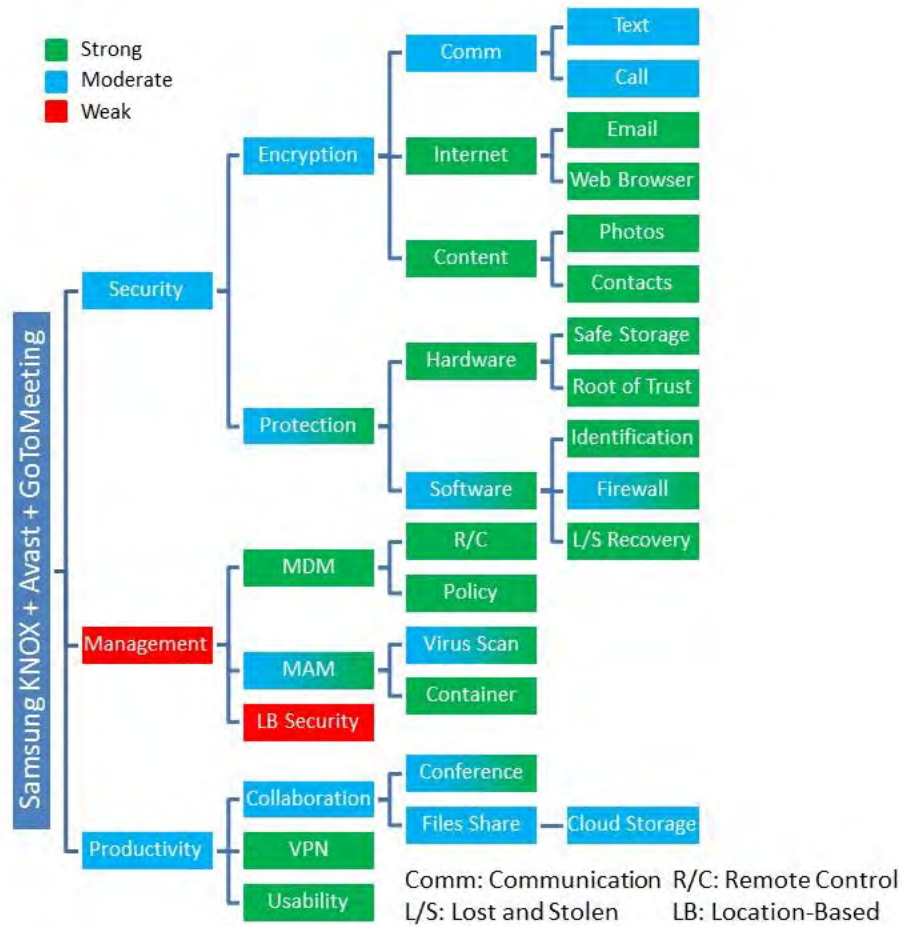
Figure 9.   Samsung Knox Functional Analysis

b.   *HTCpro Android*

HTCpro is a certification provided by the HTC Corporation to promote its enterprise-ready smartphone products. The HTCpro certified Android OS features data encryption technology, MDM, and VPN functions to improve the Android mobile security. It also provides various applications, including email, calendar, notes, online storage, and Wi-Fi sharing and printing, to enhance the user's experience and productivity. [107] Table 8 summarized the HTCpro Android features with respect to security, management, and productivity.

---

[107] HTC Corporation, "The Award-Winning New HTC One Is Enterprise Ready," May 23, 2013, http://www.htc.com/us/about/newsroom/2013/2013-05-23-the-award-winning-new-htc-one-is-enterprise-ready/.

Table 8.   HTCpro Android[108]

Features and Functionality		
Security	1	Data Encryption (256-bit AES Encryption engine)
Management	1	MDM (Microsoft Exchange ActiveSync® or third-party MDM solutions)
	2	Remote lock and wipe
Productivity	1	VPN (native Android platform and third-party VPN solutions)
	2	HTC Sense®-enabled productivity capabilities—HTC BlinkFeed (customizable home screen), HTC Zoe (social app), HTC BoomSound (premium quality sound), and HTC Sense TV (TV + phone integration)
	3	Enhanced email and calendar functions including filtered email searches and cross–time-zone scheduling
	4	Wi-Fi sharing and remote printing

One significant disadvantage of HTCpro is the lack of an official endorsement. Currently, no government entity has granted the HTCpro Android approval for use. Throughout our research, we also found the lack of detailed technical specifications and explanation about the HTCpro Android alarming. This has led us to believe that the HTCpro is more of a fancy business advertisement than a real technology development. Based on the information in hand, we decided to pair the same third-party applications used in the Samsung Knox option with the HTCpro to increase its antivirus/firewall and conference call functionality. Figure 10 depicts the results of HTCpro functional analysis.

---

[108] HTC Corporation, "The Award-Winning New HTC One Is Enterprise Ready"; HTC Corporation, "HTCpro Certified," accessed March 1, 2015, http://www.htcpro.com/business-solutions.
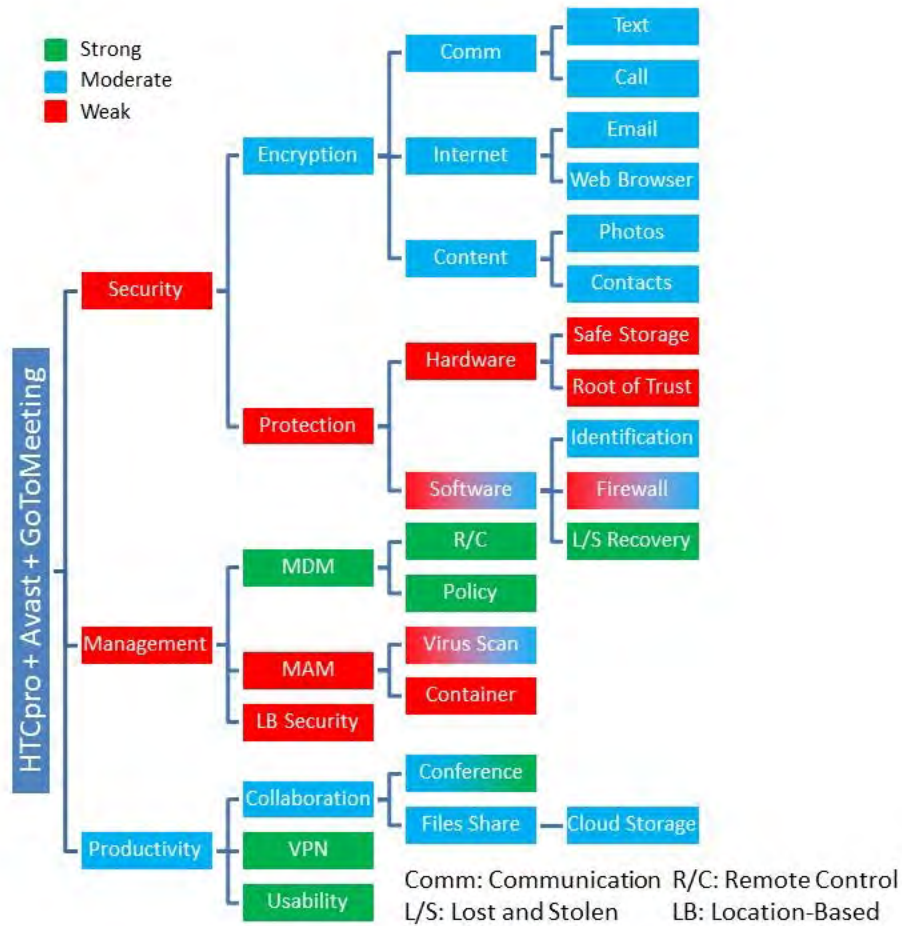
Figure 10.   HTCpro Functional Analysis

c.   *Apple iOS*

The iOS, originally iPhone OS, is the mobile operating system developed by Apple. In Chapter II we mentioned that the iOS is the most secure operating system on the market.[109] In the official Apple document, *iOS Security*, the first sentence to open the chapter reads: "Apple designed the iOS platform with security at its core," a statement validated by approval from DISA.[110] The uniqueness of iOS security is that it protects

---

[109] Timberg, "Why Surveillance Companies Hate the iPhone."

[110] Apple Inc., *iOS Security*, 4; Defense Information Systems Agency, "Secure Unclassified Mobile Devices and Wireless Services."

not only the device but the entire Apple ecosystem.[111] Referencing the iOS security publication, we summarized the features and functionality of the latest iOS in Table 9.

Table 9.   Apple iOS[112]

Features and Functionality		
Security	1	Secure boot chain—Hardware root of trust
	2	System software authorization—software integrity verification and protection
	3	Passcode and Touch ID (biometric identification—fingerprint)
	4	One dedicated AES 256-bit crypto engine
	5	Effaceable Storage—deep level data erasure against data remnant exploit
	6	App code signing—Apple App store review and certification
	7	App sandboxing
	8	Apple ID
Management	1	Single Sign-on
	2	MDM Capabilities—Passcode management, configuration enforcement, device enrollment program, Apple configurator, device restrictions, and supervised-only restrictions
	3	Remote wipe
	4	Find My iPhone and Activation Lock—device location tracking and remote lock
	5	Privacy control
Productivity	1	SSL, TLS, DTLS, and VPN—Network security*
	2	AirDrop—secure files transfer/share (2048-bit RSA identity hash)
	3	iMessage (RSA 1280-bit encryption key and ECDSA 256-bit signing key)
	4	FaceTime—video and audio calling service (AES 256-bit encryption)
	5	iCloud—online storage (AES 128-bit encryption and SHA 256-bit hash)
	6	Handoff—work/task continuity**
	7	Hotspot—Internet connectivity sharing
*SSL: Secure Socket Layer, TLS: Transport Layer Security, DTLS: Datagram Transport Layer Security **Continuity features allow seamlessly work/task transfer between iOS devices (features may vary by different system requirements)		

---

[111] Apple Inc., *iOS Security*.

[112] Ibid.

Overall, Apple iOS has strong performance across the functionality chart depicted in Figure 11 except for location-based security. Although many MDM/MAM solutions provide security policy enforcement or application disablement, the inability to carry out location-based execution is the biggest obstacle for productivity and security management. Better management that can satisfy both productivity and security demands requires finer-grained control over location-based information. Since Apple iOS meets most of the desired functions, it does not need third-party applications to remediate its functionality. However, for comparative analysis, we decided to use Google Drive for larger free online storage capacity (15 GB vs 5 GB on iCloud) and GoToMeeting for conference calls across different mobile platforms and operating systems.
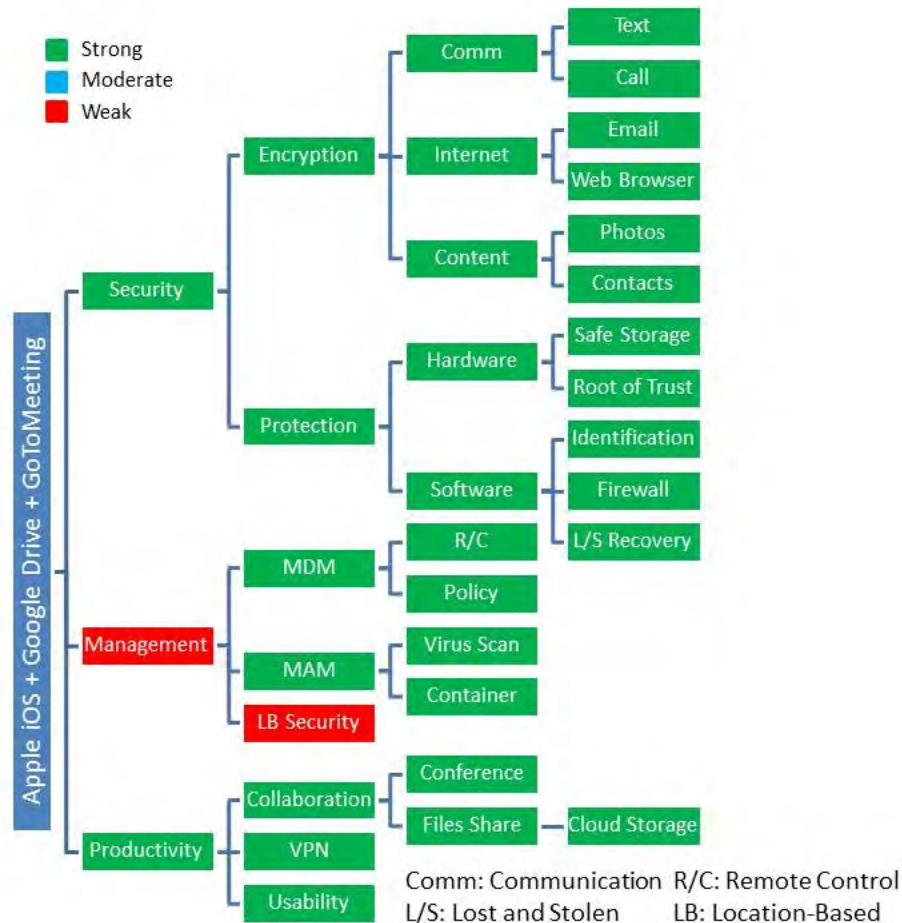

Figure 11.   Apple iOS Functional Analysis

d. *BlackBerry 10 OS*

BlackBerry Limited, formerly Research In Motion (RIM) Limited, was known for its first portable email device back in 1999.[113] Throughout the early 2000s, it became the indispensable accessory of business executives and heads of states until the introduction of iPhone and Android.[114] Although BlackBerry's Taiwan market share is insignificant compared to other popular smartphone makers and its recent business strategy shift in focus from device to software, BlackBerry is still the world leader in the enterprise mobility products and services.[115] The latest mobile platform released by BlackBerry, the BlackBerry 10, features various productivity and security features, such as hardware root of trust, MDM/MAM, data-in-transit/at-rest security, task/note/memo organization, and centralized emails/messages control.[116] Referencing various BlackBerry official websites and publications, we summarized the features and functionality of the latest BlackBerry 10 OS in Table 10.

---

[113] BlackBerry Limited, "BlackBerry Charts New Course by Officially Adopting Its Iconic Brand Name," July 10, 2013, http://press.blackberry.com/press/2013/blackberry-brand-name.html; Kevin C. Tofel, "BlackBerry: The One Time Smartphone Leader, Its Fall, and the Comeback That Never Happened," Octover 1, 2013, GigaOM Media, https://gigaom.com/2013/10/01/blackberry-the-one-time-smartphone-leader-its-fall-and-the-comeback-that-never-happened/.

[114] Felix Gillette, Diane Brady, and Caroline Winter, "The Rise and Fall of BlackBerry: An Oral History," Bloomberg, December 5, 2013, http://www.bloomberg.com/bw/articles/2013-12-05/the-rise-and-fall-of-blackberry-an-oral-history#p1.

[115] International Data Corporation, "IDC Taiwan," March 18, 2014, http://www.idc.com.tw/about/433.html; Forbes, "New BlackBerry Smartphones Signal Shift in Focus to Enterprise Services and BBM," February 28, 2014, http://www.forbes.com/sites/greatspeculations/2014/02/28/new-blackberry-smartphones-signal-shift-in-focus-to-enterprise-services-and-bbm/.

[116] BlackBerry, *BlackBerry Security Overview* (Waterloo, Ontario: BlackBerry, March 2015), http://help.blackberry.com/en/blackberry-security-overview/latest/blackberry-security-overview-pdf/Security_Overview_BlackBerry_en.pdf; BlackBerry, "BlackBerry 10 Re-Designed Re-Engineered and Re-Invented," January 30, 2013, http://press.blackberry.com/press/2013/blackberry-10-re-designed-re-engineered-and-re-invented.html.

Table 10.   BlackBerry 10 OS[117]

Features and Functionality		
Security	1	Hardware root of trust—trusted computing/attestation
	2	BlackBerry Guardian—App vetting (Allowed/Disallowed App List)
	3	Passcode and two-factor authentication (smart cards)
	4	Microkernel architecture—less exposure to kernel exploits/attacks[118]
	5	Data-in-transit security—designated BlackBerry infrastructure and AES 256-bit encryption
	6	Date-at-rest security—AES 256-bit encryption
	7	App sandboxing
	8	Internal and external storage encryption[119]
Management	1	BlackBerry Protect—remote location tracking, lock, password reset, wipe
	2	BlackBerry Blend—remote access/work continuity
	3	BlackBerry Balance—MDM/MAM (including NAC*)
	4	BES 12—Cross-platforms (iOS, Android, Windows Phone, Samsung Knox and BlackBerry devices) Enterprise Mobility Management by BlackBerry[120]
Productivity	1	VPN
	2	BBM—secure messaging service
	3	BBM Meeting—mobile collaboration
	4	Amazon Appstore—Android Apps downloads**
*Network Access Control **BlackBerry 10 OS can run Android Apps that are being securely controlled (App sandboxing and containerization, review, and certification)[121]		

---

[117] BlackBerry, *BlackBerry Security Overview.*

[118] QNX Software Systems, "QNX Neutrino Realtime Operating System," accessed March 3, 2015, http://www.google.com/ url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CDoQFjAD&url=http%3A%2F%2Fwww.qnx.com%2Fdownload%2Fdownload%2F8117%2FQNX%2520Neutrino.pdf&ei=r6Y2VYqGFsS4ogTunYCABQ&usg=AFQjCNG-u9U_Uo4BFdOFCjRe2W-qWBlDxg&sig2=X4i2771R6fG8APu6sFtTrg&bvm=bv.91071109,d.cGU.

[119] BlackBerry, "How to Encrypt Internal and External File Systems on BlackBerry Smartphones," last modified August 26, 2014, http://btsc.webapps.blackberry.com/btsc/ viewdocument.do?externalId=KB16088&sliceId=2&cmd=displayKC&docType=kc&noCount=true&ViewedDocsListHelper=com.kanisa.apps.common.BaseViewedDocsListHelperImpl.

[120] BlackBerry, "BlackBerry Enterprise Service 12," accessed March 3, 2015, http://us.blackberry.com/ enterprise/products/bes12.html.

[121] Michael Cobb, "BB10 Security: The Risks of Running Android Apps on BlackBerry 10," TechTarget, June 2013, http://searchsecurity.techtarget.com/answer/BB10-security-The-risks-of-running-Android-apps-on-BlackBerry-10.

The BlackBerry may not be one of the more popular smartphone choices for the public, but it is indeed the most popular smartphone choice for government agencies and regulated industries such as financial and healthcare services.[122] By focusing more on the Enterprise Mobility Management (EMM) capability development, BlackBerry has transformed itself from a phone maker to EMM service provider. Its BES 12, a cross-platform EMM solution, is by far the most impressive and powerful MDM/MAM solution and allows better mobile strategic options (BYOD, COPE, CYOD, and COBO), execution, and user experience. The Connect to Dropbox and GoToMeeting are our chosen third-party applications for the BlackBerry option.[123] The former is for better work productivity and larger online storage, and the latter is for easier and popular conference/meeting calls in general use. Same as all three previous analyzed smartphones, the location-based security feature is absent from the BlackBerry 10 OS. Figure 12 depicts the results of BlackBerry 10 OS functional analysis.

---

[122] BlackBerry, "Enterprise-Grade Security for Regulated Industries," accessed March 3, 2015, http://us.blackberry.com/enterprise/solutions/regulated-industries.html.

[123] BlackBerry, "BlackBerry World," accessed March 3, 2015, http://appworld.blackberry.com/webstore/viewAll/L3Byb2R1Y3R0eXBlL2FwcHMvbGlzdHR5cGUvcG9wdWxhcg%253D%253D/?lang=en&countrycode=US.
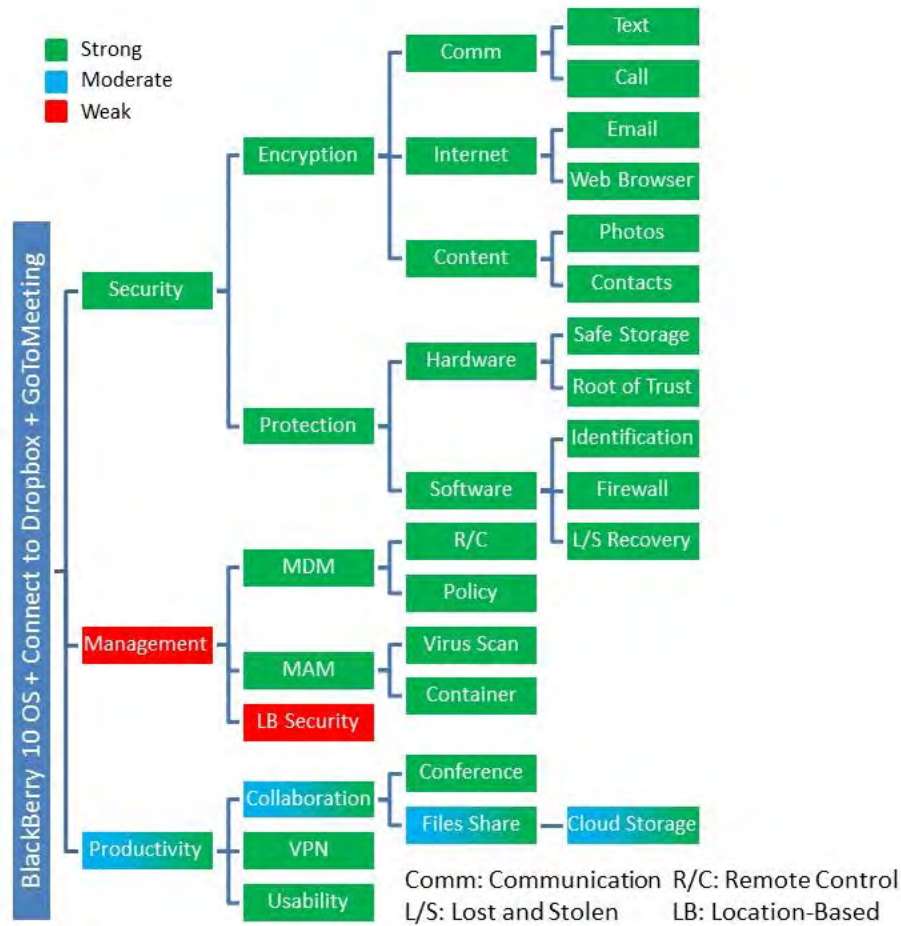
Figure 12.   BlackBerry 10 OS Functional Analysis

2.   Recommended Option

The analysis reveals that Apple iOS is the most secure and productive system for smartphone incorporation in the Taiwan navy. It shows strong performance across the functionality chart except the location-based security management, which requires more than a combination of a smartphone and applications to achieve acceptable performance and practicality. The second best option is BlackBerry, which shows the same performance as Apple iOS only after combining it with third-party applications. Although the BlackBerry misses the Apple iOS only by not having its own cloud storage service, which is a minor productivity issue, its marginal market share, which creates insignificant supportability, in the Taiwan smartphone market is in fact the deciding factor to rank the Apple iOS over the BlackBerry. Table 11 quantifies the findings of functional analyses.

All four options score only one point at management area due to the lack of location-based security management function.

Table 11.   Analysis Summary

	Rank	Security	Management	Productivity	Total
1	Apple iOS	3	1	3	7
2	BlackBerry	3	1	3	7
3	Samsung Knox	2	1	2	5
4	HTCpro	1	1	2	4
The scoring is based on the results of functional analysis in three key areas Strong performance: 3 points, medium performance: 2 points, and weak performance: 1 point					

Modern smartphones are capable of using GPS, WLAN, and Cell ID signals to provide users with location-based and geosocial services such as navigation, proximity-based marketing, location tracking, and travel information.[124] Current studies show that the positioning accuracy in smartphones depends on various factors including weather conditions, the operating system, and the positioning scheme (single vs. hybrid).[125] Generally, smartphones can get within 5 to 8 meters accuracy that can be improved to 2 to 3 meters by incorporating external Bluetooth GPS receivers.[126] Nevertheless, using location-based information to build an effective and practical security management requires higher and constant positioning accuracy. Otherwise, the inadequate and inconsistent accuracy will result in high security risk and low usability.

An intriguing significance of location-based security is that theoretically, it can relieve smartphone users' burden and inconvenience in the dual persona use case, which

---

[124] Christine Bauer, "On the (In-) Accuracy of GPS Measures of Smartphones: A Study of Running Tracking Applications," paper presented at the 11th International Conference on Advances in Mobile Computing & Multimedia (MoMM2013), Vienna, Austria, December 2013; Kathryn Zickuhr, "Three-Quarters of Smartphone Owners Use Location-Based Services," Pew Research Center, May 11, 2012, http://www.pewinternet.org/2012/05/11/three-quarters-of-smartphone-owners-use-location-based-services/; Ryan Goodrich, "Location-Based Services: Definition & Examples," *Business News Daily*, October 30, 2013, http://www.businessnewsdaily.com/5386-location-based-services.html.

[125] Bauer, "On the (In-) Accuracy of GPS Measures of Smartphones."

[126] Community Health Maps, "How Accurate is the GPS on My Smart Phone (Part 2)," July 7, 2014, http://communityhealthmaps.nlm.nih.gov/2014/07/07/how-accurate-is-the-gps-on-my-smart-phone-part-2/.

requires user to adopt dual mobile operating environments, and allow finer-grained smartphone security implementation. Imagine having a smartphone that is capable of disabling camera and microphone upon entering a combat information center and resuming normal settings upon exit. Imagine a smartphone that switches to work mode at the office and switches to personal mode during a lunch break at a local Starbucks. Recently, Google and Apple both applied for new patents involving location-based (location-sensitive) security features[127] aimed at improving security implementation and user experience.

However, the location-based security service is a double-edged sword. In order to implement appropriate geo-sensitive security measures, users need to be located and tracked constantly, which poses serious threats to privacy issues such as unauthorized access to personal information and force locations/movements. In addition, a smartphone alone is unlikely to support reliable smartphone positioning for security implementation due to its limited computing power and system resources. Therefore, realizing intuitive and intelligent location-based security services depends on how to overcome privacy concerns effectively and how to locate smartphones accurately so that it truly reduces instead of escalating anxiety regarding smartphone security.

E.   MARITIME MOBILITY

Maritime mobility is a concept used to describe the capability to establish wireless network connections for mobile devices in maritime environments. To make the Taiwan navy a truly mobile enterprise both ashore and at sea, a secure, productive mobile device is not enough. Especially in order to leverage smartphones at sea, the Taiwan navy needs a way to connect the device to the rest of the world. It needs satellite and wireless communication at sea as a backhaul to the smartphone connectivity. That being said, the productivity enhancements offered by the adoption of smartphones may be in-part

---

[127] Alex Colon, "Google's Location-Based Security System Can Protect Your Phone Whenever You Leave the House," GigaOM Media, August 22, 2013, https://gigaom.com/2013/08/22/googles-location-based-security-system-can-protect-your-phone-whenever-you-leave-the-house/; Jack Purcher, "Apple Invents Intelligent Location-Based Security for Home & CarPlay," Patently Apple, July 3, 2014, http://www.patentlyapple.com/patently-apple/2014/07/apple-invents-intelligent-location-based-security-for-home-carplay.html.

realized with the devices being used as terminals to onboard systems, subject to approval by the overriding security policy.

The vastness and remoteness of the ocean are the challenges all navies face while trying to stay connected. The ocean carries the ships and connects the world. However, it does so in the physical domain, not in the information domain where the maritime mobility resides. The U.S. Navy has been expanding its maritime mobility since 2008 when it attempted to establish a wireless ship-to-shore connection system to 2013 when it set the goal to bring Wi-Fi and 4G LTE networks to ships and submarines.[128]

The differences in operational environment and characteristics have forced the Taiwan navy to approach maritime mobility differently. It does have capable maritime mobility for military tactical networks, ranging from encrypted ship-to-shore Wi-Fi connection to satellite command and control (C2) tactical networks. However, the maritime mobility for commercial networks is almost nonexistent due to security concerns and maritime environmental challenges the U.S. Navy also faced.[129] The maritime mobility for commercial network consists of two key nodes: satellite and wireless area communication node.

1. Satellite Communication

The idea of satellite communication (SATCOM) started from a Royal Air Force (RAF) electronic officer named Arthur C. Clarke who described the possibility of SATCOM in his short article published in 1945 in *Wireless World*.[130] Today, exactly 70 years from the very beginnings of SATCOM, there are more than 600 operational

---

[128] Heather Meredith et al., "Navy Ship-to-Shore via Wireless Connection," *CHIPS* 26, no. 4 (October–December 2008): 58; Sam Fellman, "Wi-Fi Coming To U.S. Ships, Subs," *Defense News*, October 16, 2013, http://archive.defensenews.com/article/20131016/DEFREG02/310160016/Wi-Fi-Coming-US-Ships-Subs; Greg Crowe, "Navy's Ship-to-Ship Communications Go 4G," Government Computer News, March 11, 2013, http://gcn.com/articles/2013/03/11/navy-4gs-ship-to-ship-communications.aspx.

[129] Crowe, "Navy's Ship-to-Ship Communications Go 4G."

[130] David J. Whalen, "Communications Satellites Short History," National Aeronautics and Space Administration, accessed March 6, 2015, http://history.nasa.gov/satcomhistory.html.

satellites listed for communication use that collectively provide worldwide coverage.[131] Unlike the United States, Taiwan does not have dedicated military communication satellites and only has part ownership of one commercial communication satellite, ST-2, which provides services for both commercial and military communications.[132] This does not mean that the Taiwan navy should not rely on commercial satellites for military applications. In fact, commercial satellites currently support approximately 40% of the U.S. DOD SATCOM demands, which are estimated to grow by 68% over the next decade.[133]

a. Current Development

Satellites with different purposes operate at different frequencies. Figure 13 shows that typical SATCOM transmissions use frequencies that range from 1 to 40 GHz. Within the frequency range, designations have been developed for easier reference.[134]

[131] Union of Concerned Scientists, "UCS Satellite Database," accessed March 6, 2015, http://www.ucsusa.org/nuclear_weapons_and_global_security/solutions/space-weapons/ucs-satellite-database.html#.VPnvAeGraVA.

[132] SatBeams.com, "Satellite Details—ST 2," accessed March 6, 2015, https://www.satbeams.com/satellites?norad=37606.

[133] Defense Business Board, *Taking Advantage of Opportunities for Commercial Satellite Communications Services* (Report FY13-02) (Washington, DC: Defense Business Board, January 24, 2013), http://dbb.defense.gov/Portals/35/Documents/Reports/2013/FY13-02%20Taking%20Advantage%20of%20Opportunities%20for%20Commercial%20Satellite%20Communications%20Services.pdf.

[134] European Space Agency, "Satellite Frequency Bands," November 21, 2013, http://www.esa.int/Our_Activities/Telecommunications_Integrated_Applications/Satellite_frequency_bands.

Figure 13.   SATCOM Frequency Designations[135]

Due to the increasing demands for SATCOM, congestion has become a serious issue in the earlier developed lower frequency bands (L, S, and C). To meet the market demands, the SATCOM industry has been using the higher frequency bands such as Ku (12–18 GHz) and Ka (26–40 GHz) for broader bandwidth access.[136] Currently, the SATCOM industry is using the Ku and Ka bands to develop better, more efficient, and higher performance satellites, called high-throughput satellites (HTS). The HTSs use multiple spot-beam antennas and frequency reuse mechanisms to provide five to ten times the capacity of traditional satellites. This is equivalent to a data rate increase of upward to 100 Mbps to a single site.[137] Table 12 provides the ITC Global summary of four of the more prominent HTS satellite systems emerging on the market.

[135] Ibid.

[136] Ibid.

[137] Harris CapRock Communications, *Not All Bands Are Created Equal: A Closer Look at Ka & Ku High Throughput Satellites* (Houston, TX: Harris CapRock Communications), accessed March 11, 2015, http://www.harriscaprock.com/downloads/HarrisCapRock_WhitePaper-Ka-Ku_Analysis.pdf.

Table 12. Prominent HTS Satellite Systems[138]

	1 INTELSAT. Epic[NG]	2 inmarsat Global Xpress	3 O3b Networks	4 Telesat VANTAGE
Orbit Type & Path Altitude	Great Earth Orbit (GEO) Geosynchronous 35,786 kilometers	Great Earth Orbit (GEO) Geosynchronous 35,786 kilometers	Medium Earth Orbit (MEO) Circular 8,063 kilometers	Great Earth Orbit (GEO) Geosynchronous 35,786 kilometers
Frequency Bands	Ku and C initially Ka in the future	Ka	Ka	Ku
Coverage Area	Global coverage available through traditional C and Ku satellites[139]	Global except the poles	Global limited to between 45°N and 45°S latitudes	Large areas of Americas, Africa, and Middle East including regional waters plus South Atlantic aeronautical routes
Initial Number of Satellites	2	3	8	1
Network Architecture	Open Source Backward Compatible	Proprietary Network	Proprietary Network	Open Source Backward Compatible
Advantages	Uses proven and lower cost Ku satellite antennas	Built-in L band backup capability through legacy Inmarsat service	Lower latency of 120ms compared to 650ms of GEO satellites[140]	Uses proven Ku satellite antennas. Excellent coverage area for energy and mining markets
Trade-offs	Longest lead time before satellites are in service. Does not cover all open ocean regions	Contented network primarily pre-packaged service. Some beams will not be available	Require 2 full tracking antennas even for fixed site locations	Longest lead time to availability
Anticipated Availability	2015 (IS-29e) 2016 (IS-33e)	2013 (regional) 2014 (global)	2014	2016 (Telstar 12V)

For information purposes only. All data is from publically available sources. Intelsat Epic, Inmarsat Global Xpress, O3b, and Telesat VANTAGE are trademarks of their respective owners. No endorsement or commentary implied.

[138] ITC Global, "High Throughput Satellites," accessed March 11, 2015, http://www.itcglobal.net/high-throughput-satellites.htm.

[139] Intelsat, "Intelsat Epic[NG®] Coverage," accessed April 27, 2015, http://www.intelsat.com/infrastructure/intelsat-epicng/coverage/.

[140] O3b Networks, *What Is Network Latency and Why Does It Matter?*, accessed April 27, 2015, http://www.o3bnetworks.com/wp-content/uploads/2015/02/white-paper_latency-matters.pdf.

b.   Battle of Bands: Ka vs. Ku

The debate over Ka band versus Ku band is intense, and each side provides valuable arguments on why one is better than the other to serve as the future SATCOM solution. In short, the Ka SATCOM technology is newer, but it also means that the Ku has more SATCOM infrastructure in place. The higher frequency of Ka band allows higher throughput, but it also means that the Ku has better resistance to atmospheric interference. However, as John Ashworth, the O3b Networks' principal engineer stated, "Debates about one band versus another distract us from focusing on how best to make use of this rich range of resources to best serve our communications needs."[141] To the Taiwan navy, understanding the difference between the Ka and Ku band is beneficial to understanding SATCOM development, but it should not occupy the decision process of choosing the best SATCOM options for the Taiwan navy.

c.   SATCOM Options for the Taiwan Navy

When we look into SATCOM options for the Taiwan navy, we are specifically referring to satellite Internet access or so called IP communications over satellite. There are two popular options for global access: BGAN (Broadband Global Area Network) and VSAT (Very Small Apertures Terminals).[142] BGAN uses Inmarsat I-4 constellation, and VSAT operates on other satellite carriers to provide reliable Internet connections to remote locations worldwide.[143] Strictly speaking, the Taiwan navy is a green water navy. However, it is fully capable of executing blue water missions that may demand SATCOM to enhance C2 capability. In Table 13, we listed some of the main differences between BGAN and VSAT to help the Taiwan navy determine which of the two options is best suited for its specific situations and requirements.[144] As typical commercial network consumers expect upward of 10 MB per second connection service, neither of

---

[141] John Ashworth, "The 'Great' Debate: Ka-Band versus Ku-Band," *O3b Networks* (blog), January 9, 2013, https://o3bnetworks.wordpress.com/2013/01/09/the-great-debate-ka-band-vs-ku-band/.

[142] Network Innovations, "BGAN or VSAT—Comparing the Technologies," April 26, 2012, http://www.networkinv.com/bgan-or-vsat-comparing-the-technologies/.

[143] Ground Control, "BGAN Coverage Map," February 24, 2015, http://www.groundcontrol.com/bgan_coverage_map.htm; Network Innovations, "BGAN or VSAT—Comparing the Technologies."

[144] Ibid.

these services would satisfy consumer demand on a continuous basis. However, the rates offered by these services are within the demands for operational requirements.

Table 13.   BGAN vs. VSAT[145]

	BGAN	VSAT
Data Volumes	Better for short-term small amount of data transfer	Better for long-term large amount of data (hundreds of megabytes or gigabytes) transfer
Link Speed	Standard/Shared IP: peak 490Kbps* Streaming/Dedicated IP: selectable 32 to 384Kbps	Selectable 64Kbps to multiple Mbps
Number of Concurrent Users	Better for single user or small teams who have sporadic usage patterns	Better for large operations with multiple users and continuous usage patterns
Capital Cost	Directional antennas: US$3,000 to 5,000 Auto-tracking units: US$8,000 to 18,000	Cost varies dramatically Entry level: US$3,000 but can be tens of thousands for large operations Auto-pointing system: US$20,000 to 200,000
Operating Cost	US$3 to 7 per Megabyte of data transfer/received	Often fixed monthly fee: US$200 to 20,000 per month based on bandwidth
Coverage	Seamless near global network except poles	Similar to BGAN coverage but need separate satellite network contracts to achieve global coverage
Ease of Use	Simple and easy to use, customer installable, no technician required	Trained technician required for installations
Form Factor	BGAN is about laptop computer size and includes rechargeable batteries for operation	1 to 2.4 m diameter** VSAT for most applications and needs to be tethered to a power source for operation
Communications On the Move	Best option for land use applications (smaller antennas for moving vehicles)	Best option for maritime use applications (larger antennas for underway ships)
Licensing	Less expensive in general	More expensive in general
*On February 2, 2015 Inmarsat launched the second HTS for its Global Xpress constellation that brings consistent high-speed connectivity of up to 50 Mbps on download and 5Mbps on upload[146] ** World's smallest VSAT is the KVH TracPhone V3 measuring just 37cm in diameter[147]		

[145] Ibid.

[146] Jonathan Amos, "Inmarsat Launches Second Global Xpress Satellite," British Broadcasting Corporation, February 2, 2015, http://www.bbc.com/news/science-environment-31097265; Inmarsat and IEC Telecom, *Global Xpress*, accessed March 11, 2015, http://www.iec-telecom.com/wp-content/uploads/2014/09/iec_telecom_datasheet_global_xpress_service_v5.pdf.

[147] KVH Industries, Inc., "KVH's New TracPhone V3, World's Smallest Ku-Band Maritime VSAT Terminal, Receives FCC License," April 27, 2011, http://www.kvh.com/Press-Room/Press-Release-Library/2011/110427-V3-Licensed-Shipping.aspx.

2. Wireless Area Communication

The Taiwan navy has always worked hard to establish reliable and efficient communication networks such as HF, VHF, UHF, and tactical data links to deployed vessels. Although these networks prove useful and reliable most of the time, they also have clunky terminals that require skilled sailors to operate. Commercial wireless networking technology can dramatically improve current network efficiency and ease training requirements for operators. However, it is not to supplant but to supplement existing naval tactical networks.[148]

Embracing commercial wireless networking technology in naval environments has many potential benefits depending on the wireless network area size. Furthermore, the wireless networking technology can expand SATCOM footprints without installing expensive SATCOM terminals on every ship in the Taiwan navy. Table 14 shows a short list of current popular COTS wireless networking technologies and potential applications in the Taiwan navy.

---

[148] Spencer Ackerman, "In First, Navy Will Put 4G Network on Ships," *Wired*, May 23, 2012, http://www.wired.com/2012/05/navy-wwan/.

Table 14.   Wireless Networking Benefits

Area Size[149]	Technology	Naval Application
1 to 10 meters (WPAN)*	Bluetooth	Onboard mobile devices mirroring, direct files sharing/transfer and audio/video streaming
	Wi-Fi Direct	
	LTE Direct	
10 to 107 meters (WLAN)	Wi-Fi	Shipwide network connection and Internet/intranet access, in port ship-to-shore network connection
107m to 56km (WMAN)	WiMAX	Underway SAG**, ship-to-ship, ship-to-air network connection, audio/video streaming, expand SATCOM Internet/intranet coverage
longer than 56km (WWAN)	4G LTE	
*WPAN (Wireless Personal Area Network), WLAN (Wireless Local Area Network), WMAN (Wireless Metropolitan Area Network), and WWAN (Wireless Wide Area Network) **SAG (Surface Action Group)		

After identifying the appropriate and necessary technological components to be incorporated in the Taiwan navy, there is still more to be done before creating an acceptable smartphone incorporation plan. One thing in particular is execution of a pilot program. Through the pilot program, the technological components can be further evaluated and verified. More importantly, the pilot program allows the Taiwan navy to see the role that technology plays and the limitation that technology has in the overall smartphone incorporation process in order to develop corresponding strategy, policy, and training.

---

[149] Mark D. Ciampa, *CWNA Guide to Wireless LANs,* 3rd ed. (Boston, MA: CENGAGE Learning, 2012), 21.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SMARTPHONE INCORPORATION PILOT PROGRAM

Smartphone incorporation is a reinvention, not a revolution, for the Taiwan navy's information security practice. A proper reinvention first needs a proper evaluation to justify the pros and cons. For this reason the Taiwan navy should conduct a pilot program. The pilot program's purposes are to identify any disconnect between the policy-maker and the frontline user, misunderstanding between prediction and reality, and any misalignment between the stated problem and proposed solutions. Negligence of a pilot program likely leads to an ineffective incorporation that fails to recognize deficiencies in strategy, policy, technology, and training. Ultimately, the ineffective smartphone incorporation will impair the Taiwan navy's information security practice instead of improving it. Due to the scope and investment of this study, the smartphone incorporation pilot program for the Taiwan navy is in fact only a limited objective experiment (LOE). In the *Joint Concept Development and Experimentation Campaign Plan, FY 2004–2011*, an LOE is defined as "a narrowly scoped, analytically focused concept assessment or prototype validation event. It provides final dress rehearsal of a concept or major component of a concept prior to its final validation in a full joint warfighting experiment."[150]

A. PURPOSE

The purpose of the Taiwan navy smartphone incorporation pilot program as proposed herein is to reveal the potential influence of smartphone applications upon the Taiwan navy via selected experiments that realistically represent ashore and maritime scenarios in order to assess the utility and feasibility of the smartphone incorporation.

1. Objectives

The objectives of the proposed pilot program are:

---

[150] United States Joint Force Command, *Delivering Innovation: The Joint Concept Development and Experimentation Campaign Plan FY2004–2011* (Washington, DC: United States Department of Defense, January 26, 2004), http://www.au.af.mil/au/awc/awcgate/jfcom/deliver_innov.pdf.

1. Collect data for smartphone incorporation concept assessment and influence analysis.

2. Provide the Taiwan navy with quantitative measures to answer specific research questions and operational concerns associated with smartphone incorporation.[151]

2. Participants

To account for unforeseen information and operational security risks while conducting the pilot program, we form a low-risk pilot group comprised of naval personnel of various ranks, from various units, at different levels of the Taiwan navy. Furthermore, in order to realistically represent ashore and maritime conditions, the selection of participants will be based on a complete chain of command related to a desired event. Chain of command constitutes the information flow in military operations. Participants comprised of an incomplete chain of command can reveal only an incomplete picture of the smartphone influence to the Taiwan navy. The incomplete picture often leads to a faulty assessment, which defeats the purpose of the pilot program.

B. PROGRAM

To answer the specific research questions identified in Chapter I and the operational concerns the Taiwan navy has towards smartphone incorporation, the program is comprised of three scenario-based experiments. These experiments represent the most common events seen in the Taiwan navy operations and aim to reveal the influence of security, productivity, cost, and user experience on the selection of a smartphone solution for the Taiwan navy.

1. Rules

Rules are set to establish safe boundaries for the experiments. They must be followed to ensure the credibility, reliability, and integrity of the results gathered from the experiments. Table 15 lists the rules and regulations that are developed to allow the establishment of the least risky and most realistic experimental environment.

---

[151] Ibid.

Table 15.   Rules

	Rules
1	All experiments must not involve materials that may compromise the Taiwan navy warfighting capabilities
2	All experiments should be conducted under the assumption of no subsidy
3	All smartphones involved in experiments are required to comply to the followings: • For iOS: Apply the latest software updates; jailbreak forbidden; and set up auto-lock, passcode/touch ID and Find My iPhone app • For Android: Apply the latest software updates; set up auto-lock; passcode/biometric ID, remote control app, and antivirus/firewall
4	All participants involved in experiments must agree to the following: • All smartphone data generated during the experiments are subject to monitor and analysis • All participants are allowed to take photos but forbidden to extract/upload any file or content generated during the experiment to external/cloud storage or social media. File transfer between participants is allowed. • Participants are liable for any smartphone-related misconduct that is not associated with experiments

2.   Experiments and Scenarios

We developed three scenarios to represent the most likely and current smartphone applications in the Taiwan navy. The duration of the experiment is our baseline for scenario development. First, the long-term experiment is based on an ashore scenario and lasts one month. Second, the short-term experiment is based on a maritime scenario and lasts one week. Last, the rushed experiment is based on an emergency scenario and lasts for only one day. Each experiment is comprised of four parts: scenario description, participant list, experimental objective, and deliverable data.

a.   Long-Term (Ashore Scenario—One Month)

Since the Taiwan naval force is not currently engaged in any conflict and spends more time ashore, we created a long-term experiment that aims to simulate the Taiwan navy's daily operations and activities ashore, such as situation reports (SITREPs), general administrative tasks, training coordination, and unclassified communications. Table 16 describes the long-term experiment in detail.

Table 16.   Long-Term Experiment

Long-Term Experiment	
Scenario Description	PFG-1202 has been selected as the pilot unit to conduct the Taiwan navy smartphone incorporation pilot program for 30 days. The ship is expected to stay in port and to keep up all routine tasks such as training and maintenance for the duration of the program. In addition, crew on leave forms several safety groups during the leave period, and the group leaders are to conduct safety checks and report results back to the ship no later than 1900 every day. The officer of the deck (OOD) is to deliver routine ship's SITREP that includes crew muster count, fuel/water/ammunition stock, and plan of the day (POD) at 2000 every day. Synopsis: the crew carries out usual work and personal tasks while using smartphone capabilities whenever and wherever the crew sees fit.
Participant List	PFG-1202 crew and ship's phones 124th Flotilla quarter deck and operation/training office phones
Experimental Objectives	Show smartphone impact on productivity and costs associated with daily ashore activities in the Taiwan navy Show the potential realistic security risk of the smartphone incorporation in the Taiwan navy
Deliverable Data	Participants' smartphone bill during the experiment Participants' smartphone media data (audio, photo, and video files) generated during the experiment Participant feedback during the experiment

b.   Short-Term (Maritime Scenario—One Week)

The short-term experiment aims to simulate the Taiwan navy's routine maritime operations and activities. In addition, the experiment also demonstrates commercial SATCOM capabilities using BGAN terminals. Table 17 describes the short-term experiment in detail.

Table 17.   Short-Term Experiment

Short-term Experiment	
Scenario Description	PFG-1202 is currently underway for a one-week long patrolling mission. On the third day of the mission, the ship encounters a suspicious vessel, and the CO decides to conduct aerial reconnaissance. The helicopter pilot takes photos of the suspect target and uses BGAN to transfer the images back to 124th Flotilla operations office for target verification after returning to the ship. On the fourth day, the CO grants BGAN access to the crew who want to contact their families and loved ones. Synopsis: the ship conducts a regular maritime mission while using the smartphone and commercial SATCOM capabilities whenever and wherever the CO sees fit.
Participant List	PFG-1202 crew and ship's phones 124th Flotilla quarter deck and operation/training office phones
Experimental Objective	Demonstrate the smartphone and commercial SATCOM capabilities in a maritime environment to the Taiwan navy Show smartphone and commercial SATCOM impact on crew morale
Deliverable Data	BGAN terminal usage and fee Participants' smartphone media data (audio, photo, and video files) generated during the experiment Participant feedback during the experiment

c.   *Rushed (Emergency Scenario—One Day)*

The rushed experiment aims to simulate possible emergencies in the Taiwan navy. The scenario aims to cover both maritime and ashore conditions and to show the enhanced mobility potential of smartphone incorporation and commercial SATCOM application in the Taiwan navy. Table 18 describes the rushed experiment in detail.

Table 18.   Rushed Experiment

Rushed Experiment	
Scenario Description	On the last day of the patrolling mission, PFG-1202 receives a distress call from a foreign sailboat that suffered engine failure and requires rescue. Under the CO's order, the ship rushes to the site and successfully rescues three people onboard. There is only one problem: they only speak Portuguese. With the assistance of smartphones and BGAN, the crew is able to communicate with the rescued personnel and to document the entire emergency with videos and photos. Upon returning to port, 124th Flotilla operation office prepares the necessary medications for the rescued personnel who also use the crew's smartphones to contact families and loved ones. Synopsis: the ship conducts an emergency rescue mission while using smartphones and commercial SATCOM capabilities whenever and wherever the CO sees fit.
Participant List	PFG-1202 crew and ship's phones 124th Flotilla quarter deck and operation/training office phones
Experimental Objective	Demonstrate smartphone and commercial SATCOM capabilities in an unpredictable emergency situation for the Taiwan navy Show smartphone and commercial SATCOM impact on the Taiwan navy's emergency response capability
Deliverable Data	BGAN terminal usage and fee Participants' smartphone media data (audio, photo, and video files) generated during the experiment Participants' feedback during the experiment

C.   PRODUCT

The experimental data serve as the quantitative measures to provide the Taiwan navy with initial insights and assessments of smartphone incorporation. The intent of the pilot program is to deliver three main sets of data: operation costs, device content, and participant feedback. First, the operation costs provides the Taiwan navy quantitative measures of smartphone impact on communications cost. Second, the device content, such as media files, text message/call/data usage, and application downloads, helps the Taiwan navy understand the delicate relationship of security and productivity induced by smartphone incorporation. Lastly, participant feedback provides valuable employee opinions regarding smartphone incorporation within the Taiwan navy and helps it develop a successful smartphone incorporation policy.

1. Data Analysis and Comparison

To better understand smartphone influence on security, productivity, cost, and user experience, we summarize necessary data analyses and comparisons in Table 19 to show the underlying results and implications from the experiments.

Table 19.   Data Analysis and Comparison

Influence	Data	Analysis	Comparison
Cost	Participant's smartphone bill	Cost analysis of text message, call, and data usage during the experiment to show the smartphone's impact on ashore communication expenses	Compare cost during the experiment against other regular monthly bills
Cost	BGAN terminal usage and fee	Cost analysis of BGAN usage to show the commercial SATCOM cost in maritime operation	Compare BGAN cost against estimated operations cost of same usage using military SATCOM
Security	Device contents	Analyze device content to determine the presence of content that poses threat to information and operation security	Identify areas where security was either enhanced or placed at risk
Productivity	Participant smartphone activity logs	Analyze activity logs to determine work-related communication and task completion time (efficiency)	Compare efficiency against estimated completion time of the same communication and tasks using traditional methods
Productivity	Participant smartphone activity logs	Analyze activity logs to determine applications usage and user behavior	Identify areas where productivity was either enhanced or adversely impacted
User experience	Participant feedback	Analyze participant feedback to determine the percentage of positive and negative experiences	Identify experiences that would have been similar without the smartphone incorporation

2. Evaluation Criteria and Standards

Evaluation criteria and standards serve as benchmarks to the smartphone influence to be explored by the pilot program and as a basis for guidelines to the Taiwan navy to facilitate smartphone incorporation. Based on the categories of influence or impact in the data analysis and comparison, the evaluation metrics are presented in Table 20 according to the same categories as the analysis and comparison, in a relatively simple and straightforward manner.

Table 20.   Evaluation Metrics

	Category			
	Cost	**Security**	**Productivity**	**User Experience**
Criteria and Standard	BGAN cost may not exceed military SATCOM cost while performing the same tasks	No device content should pose threat to information and operations security	Work-related communication and task completion time may not increase	Positive feedback should be more than 51%

The pilot program is intended to provide the Taiwan navy with data so as to assess whether or not smartphone incorporation poses unacceptable threats to information and operations security; its potential impact to productivity and morale; and its cost to the organization. The valuable measurements, assessments, and insights from the pilot program are necessary supports to a successful development of an effective smartphone incorporation plan that ultimately optimizes the security and productivity needed by the Taiwan navy.

V. CONCLUSIONS AND RECOMMENDATIONS

An invincible military unit is the perfect integration of security and productivity. This is the vision that all military organizations, including the Taiwan navy, have. In the Art of War, Sun Tzu wrote, "Those skilled in warfare establish positions that make them invincible."[152] To become an invincible force the Taiwan navy needs to modify its approach towards smartphone technology. Instead of denying and blockading it, the Taiwan navy should leverage and incorporate it. This research has shown that with the right combination of hardware and software, the smartphone can be secure and productive, and help the Taiwan navy become so. We understand that the Taiwan navy is willing to safeguard its information security at all cost. However, through research and analysis, we show the Taiwan navy that safeguarding information security does not necessarily mean sacrificing information productivity and connectivity. The focus on mobile security has prompted the development of various security technologies and concepts such as hardware roots of trust, application "sandboxing," and application review. These technologies spread across the five layers of the mobile security stack to establish a safe environment where everyone, including the Taiwan navy, can trust the smartphone to empower us by bringing productivity and connectivity to our fingertips, while remaining vigilant to the risks associated with all networked communications.

A. SUMMARY

The assurance of information security and operation security when incorporating smartphones into the Taiwan navy force structure is dependent on the constant improvement of the entire smartphone incorporation process, strategy, policy, technology, and training. Our research focuses on the technology piece in the process and identifies the most appropriate COTS system in the market. The advantages of the COTS approach include faster procurement and deployment, lower cost, and less technical and financial risk compared to the custom-developed approach. Another reason we favored

---

[152] Thomas Huynh, *The Art of War—Spirituality for Conflict: Annotated & Explained* (Woodstock, VT: SkyLight Paths, 2008), 51.

the COTS approach was due to the fact that most COTS systems have been designed for the consumer market and have a high rating of usability.

The Apple iOS system is the most suitable choice to start the incorporation process. Its security-oriented designs including hardware, operating system, software, and ecosystem show promise for maintaining smartphone security while supporting productivity natively. One important deficiency that the Apple iOS, and all other smartphones, has is the lack of a location-based security service. This capability is considered critical due to its potential to seamlessly manage security and productivity. The location-based security allows intuitive and finer-grained smartphone security implementation, while maximizing productivity by using the smartphone's physical location instead of a user's free will to distinguish work and personal space.

A smartphone operating without connectivity is akin to a Tesla electric car traveling without a rechargeable battery: both systems are ineffective. SATCOM proves to be the answer to bring connectivity to remote maritime environments and to enable smartphones to supplement the Taiwan navy maritime C2 capabilities. Smartphones can do so by staying connected to the Internet via SATCOM to project its capabilities towards routine and unforeseen operations at sea through various smartphone IP-based applications. In addition, the Taiwan navy can consider commercial SATCOM, whose operating cost continues to improve, as a feasible backup to its regular C2 infrastructure resources.

In the Taiwan navy, the perception of risks and benefits of smartphone incorporation varies dramatically between the two stakeholder groups. One group's benefits can often be the other's risks, and vice versa. For example, an adoptive stakeholder welcomes the productivity brought on by smartphone incorporation, but the perceived benefit can be viewed as a critical security risk by the top leadership in the organization. In contrast, the top leadership's determination to ensure total information security can become a costly barrier that restricts adoption of the smartphone's capabilities with respect to productivity, competitiveness, and initiative by the adoptive stakeholder in the information warfare age.

In the grand scheme of incorporating smartphones into the Taiwan navy force structure, a pilot program is necessary to explore the risks and assess benefits assumed by both stakeholder groups and evaluate the performance of the recommended technologies. The pilot program constructed in this study consists of three experiments that simulate common ashore activities, common at sea activities, and emergencies. Through these experiments, we propose the collection of various pieces of data such as device content, activity logs, spending records, and user feedback to reveal the influence and impact that smartphones and commercial SATCOM have on security, productivity, cost, and user experience. Ultimately, the purpose of the pilot program is to use its analytical results to help address adoption concerns and determine the possibility of smartphone incorporation in the Taiwan navy.

This research has spent a great deal of time and effort to assemble the existing COTS smartphone security-related technologies in order to provide the Taiwan navy with secure technological options. To develop an incorporation plan that ensures both information security and operation security, the recommended option alone is a convincible starting point but not a magic wand that will conjure up a fail-proof plan. Only when all aspects of the incorporation process, namely strategy, policy, technology, and training, fit with one another can we confidently trust that smartphone technology will bring a balance of security and productivity to the Taiwan navy.

B. RECOMMENDATION

Finding the right technological solutions for the Taiwan navy to build a proper smartphone approach that optimizes information security and productivity was the goal of this research. The increasingly disproportional and damaging negativity of the Taiwan local news and social media against the Taiwan military only stresses the need to further this research. There are several possible reasons for the information security incidents that have resulted from the use of smartphones. Some may in part be due to mismatch within the smartphone incorporation process or in part due to an inappropriate approach to smartphone security management. The purpose of this research was to assist the

Taiwan navy to further recognize and understand the importance of smartphones with respect to the maneuverability and their capability to enhance information age operations.

Currently, the Taiwan Ministry of Defense continues to address information security risks by instituting stricter regulations and heavier punishments that further impair its productivity and undermine the possibility of recapturing the initiative in the local information domain. To limit the Taiwan navy from entering a vicious cycle of trying to fully eliminate the security risk posed by smartphones, the Taiwan navy must leverage the existence of abundant efficient and effective smartphone device and application management tools to find the balance between security and productivity. Significantly, we discovered that the location-based security service, which is absent from all of the major smartphone operating systems, can be the critical missing piece for the Taiwan navy to establish a comprehensive environment where security is upheld, productivity thrives, and the user is satisfied. To advance the finding from this thesis, the mobile device incorporation process customization and location-based security application are the identified areas for further study.

While the Apple iOS and BlackBerry show strong performance in upholding smartphone security, the other smartphone systems can improve and strengthen their security performance with help from third-party applications, whose trending cross-platform and cloud-based movement may provide the Taiwan navy more flexible and suitable technological solutions in the near future. "Mobility first and stay connected" is a global phenomenon that the Taiwan navy cannot and should not resist. It requires the Taiwan navy to rethink its strategy, revise its policy, review its technology, and reinvent its training to construct a sound plan for smartphone incorporation. As the smartphone continues to revolutionize and deepen its roots in every aspect of day-to-day life, trying to isolate the Taiwan troops from it seems strikingly and alarmingly similar to the closed-door policy of the Qing dynasty in the eighteenth century. In order to prevent history from repeating itself, it is time for the Taiwan navy to attempt different approaches to explore the best practice of productive mobile security to chart the endless possibilities in the sea of information and to navigate its strategy towards the leading edge of information mobility.

LIST OF REFERENCES

ABI Research. "App Wrapping and Container Technologies to Drive Mobile Workspace Management Subscribers Past 60 Million by 2018." September 16, 2013. https://www.abiresearch.com/press/app-wrapping-and-container-technologies-to-drive-m/.

Absalom, Richard. *Beyond BYOD : How Businesses Might COPE with Mobility* (White paper). London: Ovum Ltd. Accessed February 12, 2015. http://us.blackberry.com/content/dam/blackBerry/pdf/business/english/Beyond-BYOD-BlackBerry-Ovum.pdf.

Ackerman, Spencer. "In First, Navy Will Put 4G Network on Ships." *Wired*. May 23, 2012. http://www.wired.com/2012/05/navy-wwan/.

AirPatrol Corporation. "ZoneDefense Location-Based Mobile Security Platform." Accessed February 28, 2015. http://airpatrolcorp.com/products/zonedefense/#zd.

Amos, Jonathan. "Inmarsat Launches Second Global Xpress Satellite." British Broadcasting Corporation. February 2, 2015. http://www.bbc.com/news/science-environment-31097265.

Apple Inc. "About App Sandbox." Accessed February 12, 2015. https://developer.apple.com/library/mac/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html.

———. "App Store Downloads on iTunes." Accessed February 11, 2015. https://itunes.apple.com/us/genre/ios/id36?mt=8.

———. *iOS Security*. October 2014. https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

———. "iPad in Business—Bring Your Own Device." Accessed February 12, 2015. https://www.apple.com/ipad/business/it/byod.html.

ARM. "TrustZone." Accessed February 28, 2015. http://www.arm.com/products/processors/technologies/trustzone/index.php.

Ashworth, John. "The 'Great' Debate: Ka-Band versus Ku-Band." *O3b Networks* (blog). January 9, 2013. https://o3bnetworks.wordpress.com/2013/01/09/the-great-debate-ka-band-vs-ku-band/.

Asia Pacific Telecom. "Introduction to APT (Asia Pacific Telecom)." Accessed February 24, 2015. http://ir.aptg.com.tw/en/APTIntroduction.htm.

Bauer, Christine. "On the (In-) Accuracy of GPS Measures of Smartphones: A Study of Running Tracking Applications." Paper presented at the 11th International Conference on Advances in Mobile Computing & Multimedia (MoMM2013), Vienna, Austria, December 2013.

Beehler, Eric. "How Mobile Antivirus Software Works and How to Know If You Need It." TechTarget. March 2014. http://searchconsumerization.techtarget.com/opinion/How-mobile-antivirus-software-works-and-how-to-know-if-you-need-it.

Berger, Gunnar. "Gartner Catalyst 2012: Is the Mobile Hypervisor the Right BYOD Approach?" Gartner, Inc (blog). August 7, 2012. http://blogs.gartner.com/gunnar-berger/gartner-catalyst-2012-is-the-mobile-hypervisor-the-right-byod-approach/.

BlackBerry. "BlackBerry 10 Re-Designed Re-Engineered and Re-Invented." January 30, 2013. http://press.blackberry.com/press/2013/blackberry-10-re-designed-re-engineered-and-re-invented.html.

———. "BlackBerry Charts New Course by Officially Adopting Its Iconic Brand Name." July 10, 2013. http://press.blackberry.com/press/2013/blackberry-brand-name.html.

———. "BlackBerry Enterprise Service 12." Accessed March 3, 2015. http://us.blackberry.com/enterprise/products/bes12.html.

———. *BlackBerry Security Overview*. Waterloo, Ontario: BlackBerry. March 2015. http://help.blackberry.com/en/blackberry-security-overview/latest/blackberry-security-overview-pdf/Security_Overview_BlackBerry_en.pdf.

———. "BlackBerry World." Accessed March 3, 2015. http://appworld.blackberry.com/webstore/viewAll/L3Byb2R1Y3R0eXBlL2FwcHMvGlzdHR5cGUvG9wdWxhcg%253D%253D/?lang=en&countrycode=US.

———. "Enterprise-grade Security for Regulated Industries." Accessed March 3, 2015. http://us.blackberry.com/enterprise/solutions/regulated-industries.html.

———. "How to Encrypt Internal and External File Systems on BlackBerry Smartphones." Last modified August 26, 2014. http://btsc.webapps.blackberry.com/btsc/viewdocument.do?externalId=KB16088&sliceId=2&cmd=displayKC&docType=kc&noCount=true&ViewedDocsListHelper=com.kanisa.apps.common.BaseViewedDocsListHelperImpl.

Blackphone. "Blackphone." Accessed February 25, 2015. https://blackphone.ch/phone/.

———. "Welcome to Blackphone." Accessed April 10, 2015. https://blackphone.ch/.

———. "What Languages Does Blackphone Support?," August 2, 2014. https://support.blackphone.ch/customer/portal/articles/1565177.

Blanchard, Benjamin S. *System Engineering Management*. 4th ed. Blacksburg, VA: John Wiley & Sons, 2008.

Boeing. "Boeing Black Smartphone." Accessed April 10, 2015. http://www.boeing.com/defense/boeing-black/index.page.

Boyle, Mike. "Trusted Computing Standards Overview." National Security Agency. October 4, 2012. http://scap.nist.gov/events/2012/itsac/presentations/day2/4Oct_1145am_Boyle.pdf.

Chandramouli, Ramaswamy. *Security Recommendations for Hypervisor Deployment*. Gaithersburg, MD: National Institute of Standards and Technology. October 2014. http://csrc.nist.gov/publications/drafts/800-125a/sp800-125a_draft.pdf.

Chen, Lily, Joshua Franklin, and Andrew Regenscheid. *Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)*. Gaithersburg, MD: National Institute of Standards and Technology. October 2012. http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf.

Ciampa, Mark D. *CWNA Guide to Wireless LANs*. 3rd ed. Boston, MA: Cengage Learning, 2012.

Cisco Systems Inc. "Cisco Visual Networking Index : Global Mobile Data Traffic Forecast Update, 2010–2015," February 3, 2015. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.

Citrix Systems Inc. *Jump Start Mobile Productivity with MDM and Secure File Sharing*. Fort Lauderdale, FL: Citrix. Accessed February 11, 2015. https://www.citrix.com/content/dam/citrix/en_us/documents/oth/jump-start-mobile-productivity-with-mdm-and-secure-file-sharing.pdf.

Cobb, Michael. "BB10 Security: The Risks of Running Android Apps on BlackBerry 10." TechTarget. June 2013. http://searchsecurity.techtarget.com/answer/BB10-security-The-risks-of-running-Android-apps-on-BlackBerry-10.

Colon, Alex. "Google's Location-Based Security System Can Protect Your Phone Whenever You Leave the House." GigaOM Media. August 22, 2013. https://gigaom.com/2013/08/22/googles-location-based-security-system-can-protect-your-phone-whenever-you-leave-the-house/.

Community Health Maps. "How Accurate is the GPS on My Smart Phone (Part 2)." July 7, 2014. http://communityhealthmaps.nlm.nih.gov/2014/07/07/how-accurate-is-the-gps-on-my-smart-phone-part-2/.

Crowe, Greg. "Navy's Ship-to-Ship Communications Go 4G." Government Computer News. March 11, 2013. http://gcn.com/articles/2013/03/11/navy-4gs-ship-to-ship-communications.aspx.

Defense Business Board. *Taking Advantage of Opportunities for Commercial Satellite Communications Services* (Report FY13-02). Washington, DC: Defense Business Board, January 24, 2013. http://dbb.defense.gov/Portals/35/Documents/Reports/2013/FY13-02%20Taking%20Advantage%20of%20Opportunities%20for%20Commercial%20Satellite%20Communications%20Services.pdf.

Defense Information Systems Agency. "Secure Unclassified Mobile Devices and Wireless Services." Accessed February 27, 2015. http://www.disa.mil/Enterprise-Services/Mobility/Devices-and-Wireless-Services.

Dimensional Research. *The Impact of Mobile Devices on Information Security: A Survey of IT Professionals.* Sunnyvale, CA: Dimensional Research, June 2013. https://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf.

Dou, Eva. "Taiwan Says Phone Makers Violating Privacy Rule." *Wall Street Journal*. December 5, 2014. http://www.wsj.com/articles/taiwan-says-phone-makers-violating-privacy-rule-1417702686.

DuPaul, Neil. "Mobile Code Security." Veracode. Accessed February 11, 2015. http://www.veracode.com/products/mobile-application-security/mobile-code-security.

eBay. "SIM Card Guide." June 9, 2014. http://www.ebay.com/gds/SIM-Card-Guide-/10000000177629426/g.html.

ESD America Inc. "ESD CryptoPhone." Accessed April 10, 2015. http://esdcryptophone.com/.

European Space Agency. "Satellite Frequency Bands." November 21, 2013. http://www.esa.int/Our_Activities/Telecommunications_Integrated_Applications/Satellite_frequency_bands.

EveryiPhone.com. "Apple iPhone (Original/1st Gen/EDGE) 4, 8, 16 GB Specs." Accessed February 11, 2015. http://www.everymac.com/systems/apple/iphone/specs/apple-iphone-specs.html.

———. "Apple iPhone 6 (GSM/North America/A1549) 16, 64, 128 GB Specs." Accessed February 11, 2015. http://www.everymac.com/systems/apple/iphone/specs/apple-iphone-6-a1549-4.7-inch-gsm-north-america-specs.html.

Fellman, Sam. "Wi-Fi Coming To U.S. Ships, Subs." *Defense News*. October 16, 2013. http://archive.defensenews.com/article/20131016/DEFREG02/310160016/Wi-Fi-Coming-US-Ships-Subs.

Forbes. "New BlackBerry Smartphones Signal Shift in Focus to Enterprise Services and BBM." February 28, 2014. http://www.forbes.com/sites/greatspeculations/2014/02/28/new-blackberry-smartphones-signal-shift-in-focus-to-enterprise-services-and-bbm/.

FreedomPop. "Privacy Phone." Accessed April 10, 2015. https://www.freedompop.com/theprivacyphone.

F-Secure Labs. "Testing the Xiaomi RedMi 1S." August 7, 2014. https://www.f-secure.com/weblog/archives/00002731.html.

Gillette, Felix, Diane Brady, and Caroline Winter. "The Rise and Fall of BlackBerry: An Oral History." Bloomberg. December 5, 2013. http://www.bloomberg.com/bw/articles/2013-12-05/the-rise-and-fall-of-blackberry-an-oral-history#p1.

Goodrich, Ryan. "Location-Based Services: Definition & Examples." *Business News Daily*. October 30, 2013. http://www.businessnewsdaily.com/5386-location-based-services.html.

Google Play. "GoToMeeting—Citrix." Accessed February 28, 2015. https://play.google.com/store/apps/details?id=com.citrixonline.android.gotomeeting&hl=en.

———. "Mobile Security & Antivirus—AVAST Software." Accessed February 28, 2015. https://play.google.com/store/apps/details?id=com.avast.android.mobilesecurity&hl=en.

Ground Control. "BGAN Coverage Map." February 24, 2015. http://www.groundcontrol.com/bgan_coverage_map.htm.

Hardjono, Thomas, and Greg Kazmierczak. *Overview of the TPM Key Management Standard*. Beaverton, OR: Trusted Computing Group. Accessed February 11, 2015. https://www.trustedcomputinggroup.org/files/resource_files/ABEDDF95-1D09-3519-AD65431FC12992B4/Kazmierczak20Greg20-20TPM_Key_Management_KMS2008_v003.pdf.

Harris CapRock Communications Inc. *Not All Bands Are Created Equal: A Closer Look at Ka & Ku High Throughput Satellites*. Houston, TX: Harris CapRock Communications. Accessed March 11, 2015. http://www.harriscaprock.com/downloads/HarrisCapRock_WhitePaper-Ka-Ku_Analysis.pdf.

Haskins, Cecilia. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. 3.2.2 ed. San Diego, CA: International Council on Systems Engineering, 2011.

Huynh, Thomas. *The Art of War—Spirituality for Conflict: Annotated & Explained*. Woodstock, VT: SkyLight Paths, 2008.

HTC Corporation. "HTCpro Certified." Accessed March 1, 2015. http://www.htcpro.com/business-solutions.

———. "HTCpro Partners." Accessed February 27, 2015. http://www.htcpro.com/partners.

———. "The Award-Winning New HTC One Is Enterprise Ready." May 23, 2013. http://www.htc.com/us/about/newsroom/2013/2013-05-23-the-award-winning-new-htc-one-is-enterprise-ready/.

Infonetics Research. "Infonetics Projects Mobile Device Security Software Market to Reach $3.4 Billion in 2018." April 25, 2014. http://www.infonetics.com/pr/2014/2H13-Mobile-Security-Client-Software-Market-Highlights.asp.

Inmarsat and IEC Telecom. *Global Xpress: Global Ka Band Service*. Accessed March 11, 2015. http://www.iec-telecom.com/wp-content/uploads/2014/09/iec_telecom_datasheet_global_xpress_service_v5.pdf.

Intelsat. "Intelsat Epic$^{NG®}$ Coverage." Accessed April 27, 2015. http://www.intelsat.com/infrastructure/intelsat-epicng/coverage/.

International Data Corporation. "IDC Taiwan." March 18, 2014. http://www.idc.com.tw/about/433.html.

International Organization for Standardization. *Ergonomic requirements for office work with visual display terminals (VDTs)—Part 11: Guidance on usability*. Genève, Switzerland: ISO, 1992.

International Telecommunication Union. *The World in 2014—ICT Facts and Figures*. Geneva, Switzerland: ICT, April 2014. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf.

Investopedia. "Stakeholder." Accessed February 24, 2015.
http://www.investopedia.com/terms/s/stakeholder.asp.

ITC Global. "High Throughput Satellites." Accessed March 11, 2015.
http://www.itcglobal.net/high-throughput-satellites.htm.

Kleyman, Bill. "Hypervisor 101: Understanding the Virtualization Market." Data Center
Knowledge. August 1, 2012.
http://www.datacenterknowledge.com/archives/2012/08/01/hypervisor-101-a-
look-hypervisor-market/.

KVH Industries Inc. "KVH's New TracPhone V3, World's Smallest Ku-band Maritime
VSAT Terminal, Receives FCC License." April 27, 2011.
http://www.kvh.com/Press-Room/Press-Release-Library/2011/110427-V3-
Licensed-Shipping.aspx.

Lienemann, Ken. "Containerization: Balancing BYOD for the Enterprise and You."
Wired. June 24, 2014. http://insights.wired.com/profiles/blogs/containerization-
balancing-byod-for-the-enterprise-and-you#axzz3RTOachqw.

LinuxGizmos.com. "Article: SIM-Based WLAN Authentication for Open Platforms."
July 29, 2003. http://archive.linuxgizmos.com/sim-based-wlan-authentication-for-
open-platforms-a/.

Lutz, Zachary. "SIM-Based NFC Gains Global Support from 45 Mobile Carriers, All
Huddled around GSMA's Standard." Engadget. November 17, 2011.
http://www.engadget.com/2011/11/17/sim-based-nfc-gains-global-support-from-
45-mobile-carriers-all/.

Lynx Software Technologies Inc. "The Rise of the Type Zero Hypervisor." Accessed
February 11, 2015. http://www.lynx.com/whitepaper/the-rise-of-the-type-zero-
hypervisor/.

Malenkovich, Serge. "Rooting and Jailbreaking: What Can They Do, and How Do They
Affect Security?" *Kaspersky Lab* (blog). May 31, 2013.
http://blog.kaspersky.com/rooting-and-jailbreaking/.

Marko, Kurt. "3 Ways To Virtualize Mobile Devices—And Why You Should Do So."
InformationWeek. July 2, 2013. http://www.darkreading.com/risk-management/3-
ways-to-virtualize-mobile-devices----and-why-you-should-do-so/d/d-
id/1110613?.

Mattis, Peter. "China's Espionage against Taiwan (Part I): Analysis of Recent
Operation." *China Brief* 14, no. 21 (November 7, 2014): 4–7.

McGill, Kathleen N. "Trusted Mobile Devices: Requirements for a Mobile Trusted Platform Module." *Johns Hopkins APL (Applied Physics Laboratory) Technical Digest* 32, no. 2 (2013): 544–54.

McHale, John. "For Every Soldier, a Smartphone." Military Embedded Systems. October 9, 2013. http://mil-embedded.com/articles/for-every-soldier-smartphone/.

McNamara, Declan. "Balancing Corporate Security with User Experience." IBM. April 5, 2013. http://asmarterplanet.com/mobile-enterprise/blog/2013/04/balance-corporate-security.html.

Meredith, Heather, Greg Blanche, Jackie Mastin, and Chris Watson. "Navy Ship-to-Shore via Wireless Connection." *CHIPS* 26, no. 4 (October–December 2008): 58–59.

Mobile Work Exchange. *The 2013 Digital Dilemma Report: Mobility, Security, Productivity—Can We Have It All?* January 15, 2013. http://www.cisco.com/web/strategy/docs/gov/digital_dile_rep.pdf.

National Security Agency. "HIGH ASSURANCE PLATFORM® (HAP)." Accessed February 11, 2015. https://www.nsa.gov/ia/_files/hap_ds.pdf.

———. "NSA's First Trusted Computing Conference and Exposition." Accessed February 12, 2015. https://www.nsa.gov/public_info/media_center/ia/video/orlando2010/transcript.html.

Network Innovations. "BGAN or VSAT—Comparing the Technologies." April 26, 2012. http://www.networkinv.com/bgan-or-vsat-comparing-the-technologies/.

Ng, Raymond. "Trusted Platform Module TPM Fundamental." Infineon Technologies. August 2008. http://www.cs.unh.edu/~it666/reading_list/Hardware/tpm_fundamentals.pdf.

O3b Networks. *What is Network Latency and Why Does It Matter?* Accessed April 27, 2015. http://www.o3bnetworks.com/wp-content/uploads/2015/02/white-paper_latency-matters.pdf.

Pepin, Chris. "BYOD at IBM." IBM. January 31, 2013. http://www.slideshare.net/chrispepin/ibm-connect-2013-byod-at-ibm.

Ponemon Institute, LLC. *Security in the New Mobile Ecosystem*. Traverse City, MI: Ponemon Institute, August 2014. http://www.wincoil.us/media/89329/ponemon-raytheonsecurityinthenewmobileecosystemresearchreport.pdf.

Purcher, Jack. "Apple Invents Intelligent Location-Based Security for Home & CarPlay." Patently Apple. July 3, 2014. http://www.patentlyapple.com/patently-apple/2014/07/apple-invents-intelligent-location-based-security-for-home-carplay.html.

QNX Software Systems. "QNX Neutrino Realtime Operating System." Accessed March 3, 2015. http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CDoQFjAD&url=http%3A%2F%2Fwww.qnx.com%2Fdownload%2Fdownload%2F8117%2FQNX%2520Neutrino.pdf&ei=r6Y2VYqGFsS4ogTunYCABQ&usg=AFQjCNG-u9U_Uo4BFdOFCjRe2W-qWBlDxg&sig2=X4i2771R6fG8APu6sFtTrg&bvm=bv.91071109,d.cGU.

Qualcomm Inc. "Snapdragon Security." Accessed February 11, 2015. https://www.qualcomm.com/products/snapdragon/security.

Robinson, Brian. "Hardware-Based Mobile Security Market Heats Up." *Government Computer News*. February 10, 2014. http://gcn.com/articles/2014/02/10/mobile-hardware-security.aspx?admgarea=TC_Mobile.

Roman, Philip, Vouthanack Sovann, Kenneth Triplin, David Um, Michael Violante, and Amy Wees. "Trusted Platform Module." *ResearchedSolution* (blog). November 25, 2012. https://researchedsolution.wordpress.com/2013/09/14/trusted-platform-module/.

Rouse, Margaret. "App Wrapping (Application Wrapping)." TechTarget. July 2012. http://searchconsumerization.techtarget.com/definition/app-wrapping-application-wrapping.

————. "Hypervisor." TechTarget. October 2006. http://searchservervirtualization.techtarget.com/definition/hypervisor.

————. "Mobile Application Management (MAM)." TechTarget. June 2014. http://searchconsumerization.techtarget.com/definition/mobile-application-management.

Samsung Electronics. *An Overview of Samsung Knox* (white paper). Suwon-si, Korea: Samsung, June 2013. http://www.samsung.com/global/business/business-images/resource/white-paper/2014/02/Samsung_KNOX_whitepaper_June-0-0.pdf.

————. "Knox Workspace—Powerful Apps." Accessed February 28, 2015. https://www.samsungknox.com/en/products/knox-workspace/features/powerful-apps#Camera-and-Gallery.

————. "Knox Workspace—Technical Details." Accessed February 28, 2015. https://www.samsungknox.com/en/products/knox-workspace/technical.

———. "Samsung Knox Apps." Accessed February 28, 2015.
https://www.samsungknox.com/en/products/knox-workspace/features/apps.

———. "Samsung Knox: Business Protection. Personal Privacy. One Device." Accessed
February 28, 2015. http://www.samsung.com/us/business/samsung-for-
enterprise/downloads/KnoxBrochureSTA05_14.pdf.

SAP SE. *Bring Your Own Device (BYOD) Policy Guidebook: Questions to Ask and Best
Practices to Consider*. Accessed February 12, 2015.
http://www.emedialaw.com/files/2013/02/SAP-BYOD-Policy-Guidebook2.pdf.

SatBeams.com. "Satellite Details—ST 2." Accessed March 6, 2015.
https://www.satbeams.com/satellites?norad=37606.

Savitsky, Alex. "Weak Link: How (Not) To Lose Everything Having Lost Your SIM-
Card." *Kaspersky Lab* (blog). November 17, 2014.
http://blog.kaspersky.com/make-your-sim-secure/.

Scharr, Jill. "Blackphone vs. FreedomPop's Privacy Phone: Security Showdown." Tom's
Guide. March 7, 2014. http://www.tomsguide.com/us/blackphone-vs-
freedompop-privacy-phone,news-18427.html.

Security Research Labs. "Rooting SIM Cards." July 31, 2013. https://srlabs.de/rooting-
sim-cards/.

Skidmore, Stephen. "App Wrapping Is a Form of Containerization." Apperian. April 16,
2014. http://www.apperian.com/app-wrapping-is-a-form-of-containerization/.

Souppaya, Murugiah, and Karen Scarfone. *Guidelines for Managing and Securing
Mobile Devices in the Enterprise Revision 1*. Gaithersburg, MD: National Institute
of Standards and Technology. June 2013.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

Swaminathan, Sridher (Sree). *Mobile/NFC Security Fundamentals: Secure Elements 101*.
Princeton Junction, NJ: Smart Card Alliance. March 28, 2013.
http://www.smartcardalliance.org/resources/webinars/Secure_Elements_101_FIN
AL3_032813.pdf.

Symantec Corporation. "Infographic: Creating a Successful BYOD Policy." September
15, 2014. http://www.slideshare.net/symantec/infographic-39117177.

———. *Internet Security Threat Report 2014*. Mountain View, CA: Symantec, April 2014. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

Tapellini, Donna. "Smart Phone Thefts Rose to 3.1 Million Last Year, *Consumer Reports* Finds." *Consumer Reports*. May 28, 2014. http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.

Timberg, Craig. "Why Surveillance Companies Hate the iPhone." *Washington Post*. August 11, 2014. http://www.washingtonpost.com/blogs/the-switch/wp/2014/08/11/why-surveillance-companies-hate-the-iphone/.

Tofel, Kevin C. "BlackBerry: The One Time Smartphone Leader, Its Fall, and the Comeback That Never Happened." Octover 1, 2013. GigaOM Media. https://gigaom.com/2013/10/01/blackberry-the-one-time-smartphone-leader-its-fall-and-the-comeback-that-never-happened/.

Trusted Computing Group. "Trusted Platform Module (TPM) Summary." Accessed February 11, 2015. http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary.

Union of Concerned Scientists. "UCS Satellite Database." Accessed March 6, 2015. http://www.ucsusa.org/nuclear_weapons_and_global_security/solutions/space-weapons/ucs-satellite-database.html#.VPnvAeGraVA.

United States Department of Defense. *Defense Acquisition Guidebook*. Washington, DC: United States Department of Defense, 2013.

———. *Department of Defense Mobile Device Strategy (Version 2.0)*. Washington, DC: U.S. Department of Defense, May 2012. http://www.defense.gov/news/dodmobilitystrategy.pdf.

———. *DOD Commercial Mobile Device Implementation Plan*. Washington, DC: U.S. Department of Defense, February 15, 2013. http://www.defense.gov/news/dodcMdimplementationplan.pdf.

United States Joint Force Command. *Delivering Innovation: The Joint Concept Development and Experimentation Campaign Plan FY2004–2011*. Washington, DC: United States Department of Defense, January 26, 2004. http://www.au.af.mil/au/awc/awcgate/jfcom/deliver_innov.pdf.

Wang, Ching-i, and Ted Chen. "NCC Clears 12 Smartphone Models in Security Check." Focus Taiwan News Channel. December 30, 2014. http://focustaiwan.tw/news/ast/201412300025.aspx.

Whalen, David J. "Communications Satellites Short History." National Aeronautics and Space Administration. Accessed March 6, 2015. http://history.nasa.gov/satcomhistory.html.

Wheeler, David M. "Smartphone Security—A Holistic View of Layered Defenses." SecureComm Inc. Accessed February 11, 2015. http://www.securecommconsulting.com/downloads/NPS_Presentation_on_Smartphone_Security.pdf.

Xie, Zongxian. "Smartphone on Base Trial Verification and Control." *Youth Daily News*. January 4, 2014. http://news.gpwb.gov.tw/mobile/news.aspx?ydn=026dTHGgTRNpmRFEgxcbfcCSN9Fhd8KFbqLRgMWauV83KTHsQMjmV%2FQwBCVEb%2BKgPnpTj46r3NaVXND4iHNKfHfg3tQrsMnpfokazSjAL3k%3D.

Yoshida, Junko. "China Mobile Takes SIM Card Route to E-Wallets." *EE Times*. September 12, 2012. http://www.eetimes.com/author.asp?section_id=36&doc_id=1266182.

Zickuhr, Kathryn. "Three-Quarters of Smartphone Owners Use Location-Based Services." Pew Research Center. May 11, 2012. http://www.pewinternet.org/2012/05/11/three-quarters-of-smartphone-owners-use-location-based-services/.

INITIAL DISTRIBUTION LIST

1.   Defense Technical Information Center
        Ft. Belvoir, Virginia

2.   Dudley Knox Library
        Naval Postgraduate School
        Monterey, California